ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Análisis Comparativo de la Implementación de Voz sobre IP en Wireless Mesh Networks y Wireless LAN tradicionales tomando en consideración parámetros de Calidad de Servicio y Problemas de Movilidad ocasionados por Handoffs"

TESIS DE GRADO

Previo la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por:

Juan Carlos Basurto Dávila

GUAYAQUIL – ECUADOR

2010

DEDICATORIA

DEDICO EL PRESENTE TRABAJO
A MIS PADRES QUIENES HAN SIDO
GUIAS, AMIGOS Y UN EJEMPLO A SEGUIR.

AGRADECIMIENTO

Agradezco a Dios, por la fortaleza en todo momento
A mis padres, por su apoyo incondicional e invaluables consejos
Y a mis profesores, por compartir sus conocimientos.

DECLARATORIA EXPRESA

"LA RESPONSABILIDAD POR LOS HECHOS, IDEAS Y DOCTRINAS EXPUESTAS EN ESTE PROYECTO DE GRADUACIÓN ME CORRESPONDEN EXCLUSIVAMENTE; Y, EL PATRIMONIO INTELECTUAL DE LA MISMA, A LA ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

_____

JUAN CARLOS BASURTO DAVILA

TRIBUNAL DE SUSTENTACIÓN

ING. JORGE ARAGUNDI
SUB-DECANO DE LA FIEC

ING. REBECA ESTRADA
DIRECTOR DE TESIS DE GRADUACIÓN

ING. GERMÁN VARGAS
VOCAL

ING. CÉSAR YÉPEZ
VOCAL

RESUMEN

En los últimos años, la investigación en torno a las redes 802.11 ha ganado terreno en múltiples campos principalmente gracias a la movilidad que ofrece, entre otras ventajas. Uno de esos campos ha sido la transmisión de voz sobre el protocolo de Internet.

No obstante, añadir movilidad a redes inalámbricas supone un reto mayor para la comunicación de voz sobre IP debido a la naturaleza aleatoria del medio de propagación, expresado en los parámetros de calidad de servicio y la experiencia final del usuario.

Por otro lado, las ventajas que ofrecen las redes wireless mesh (redes amalladas inalámbricas) han popularizado su uso y su inclusión en virtualmente cualquier aplicación que se le ha dado a una red 802.11 tradicional.

El presente trabajo representa un esfuerzo por encontrar una solución disponible a los problemas de calidad de servicio experimentado en la comunicación de voz sobre redes inalámbricas en aras de optimizarla dentro de las instalaciones de la ESPOL.

Luego de realizar una revisión sobre los conceptos básicos de los elementos participantes en la presente tesis, se presentan los resultados de las pruebas efectuadas dentro de las instalaciones de la FIEC, con el objeto de probar la validez de la hipótesis planteada.

Este es el resultado del esfuerzo que se ha llevado durante el transcurso del proyecto financiado por el programa VLIR – ESPOL: “Study and design of a solution to handoff issues experimented in voice over WiFi communication optimizing quality of service prior to the IEEE 802.11r standardization”, y una motivación a continuar las investigaciones necesarias que viabilicen la implementación de voz sobre IP sobre redes 802.11 en la ESPOL.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS

AODV	Ad-hoc On-demand Distance Vector
ARP	Address Resolution Protocol
BSS	Basic Service Set
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Secuence Spread Spectrum
ESS	Extended Service Set
FHSS	Frequency Hop Spread Spectrum
IBSS	Independent Basic Service Set
IP	Internet Protocol
MAC	Media Access Control
LAN	Local Area Network
OFDM	Orthogonal Frequency Division Multiplexing
OSLR	Optimized Link State Protocol
PBX	Private Branch eXchange
PLCP	Physical Layer Convergence Procedure
QoS	Quality of Service
RTP	Real-time Transfer Protocol
SNR	Signal to Noise Ratio

TCP	Transmission Control Protocol
UDP	User Domain Protocol
VoIP	Voice over IP
VoWLAN	Voice over Wireless LAN
WEP	Wired Equivalent Security
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

INTRODUCCIÓN

En los últimos años, la investigación relacionada a las tecnologías de comunicación de voz ha ganado un interés especial en la comunicación de voz a través de las redes 802.11. Una de las motivaciones más importantes es la movilidad: la capacidad de poder desplazarse mientras existe una comunicación ha motivado tanto a la industria como a los consumidores.

No obstante, añadir movilidad trae consigo nuevos retos relacionados a la Calidad de Servicio. La transmisión de información por el medio inalámbrico supone enfrentar complicaciones como la interferencia, que termina originando problemas técnicos como la pérdida de paquetes, un delay elevado (en comparación con Ethernet), entre otros.

Sumado a estos problemas técnicos, se encuentra la limitación que data desde los orígenes de las redes 802.11: no fueron específicamente creadas para la transmisión de Voz, al contrario de las tecnologías Celulares.

Sin embargo, la movilidad y la disponibilidad de una banda no-licenciada libre y gratuita, ha motivado enormemente a la investigación, que hoy en día desarrolla nuevas soluciones para minimizar los problemas técnicos antes mencionados.

Esta tesis presenta un estudio sobre una posible solución alternativa a 802.11r, la solución Fast-handoff para las redes 802.11, con pruebas realizadas dentro de las instalaciones de la FIEC, facultad de la Escuela Superior Politécnica del Litoral.

El objetivo de este estudio es probar la eficiencia de una solución personalizada para redes Mesh (amalladas) inalámbricas en contraste con una red 802.11 WLAN tradicional y una red Mesh con equipos plug & play.

En el capítulo 1 se analizan los retos que enfrenta la implementación de Voz sobre WLAN en términos de calidad de servicio.

En el capítulo 2 se hace una revisión de los fundamentos de las Redes WLAN y Wireless Mesh (Inalámbricas Amalladas): su arquitectura, evolución, ventajas y desventajas.

En el capitulo 3 se hace una revisión sobre los fundamentos de la voz sobre IP y la voz sobre WLAN, especificando las consideraciones especiales del diseño e implementación. Se hace una revisión de la Calidad de Servicio aplicada a redes 802.11: métodos de medición, métricas y parámetros ideales.

En el capítulo 5 se realiza un análisis práctico comparativo entre la implementación de una red Voz sobre WLAN en una red tradicional y una red Mesh personalizada.

Finalmente, se exponen las conclusiones del estudio y las pruebas finales de la diferencias de la implementación de Voz sobre WLAN en una red 802.11 tradicional y una Red Mesh personalizada, bajo parámetros de Calidad de Servicio con pruebas dentro de la Facultad de Ingeniería Eléctrica y Computación de la ESPOL.

CAPÍTULO 1

1. LOS RETOS DE LA VOZ SOBRE WLAN EN TERMINOS DE LA CALIDAD DE SERVICIO Y HANDOFFS.

1.1. Antecedentes y Justificación

Desde la popularización de las redes basadas en el Protocolo de Internet y el lanzamiento oficial del Internet, la investigación relacionada a las comunicaciones ha dirigido su mirada hacia nuevas soluciones que involucren al Protocolo IP.

Como resultado, los servicios antes basados en tecnologías analógicas están siendo reemplazados por soluciones digitales basadas en IP, como en el caso de la telefonía convencional o la telefonía celular.

La voz sobre IP nace comercialmente como una solución de bajo costo de intercomunicación. No obstante, inicialmente las redes IP no fueron diseñadas para la comunicación de voz sino de datos. Caso similar, sólo que análogamente, experimentó telefonía analógica, al ser diseñada desde un principio principalmente para la comunicación de voz y no de datos, para posteriormente presentar un esquema de transimisión de datos comercial, DSL.

Sin embargo, no fue sino gracias a la implementación de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real así como la creación de estándares que permitan la calidad de servicio en redes IP que se ha podido crear las condiciones necesarias para el surgimiento y masificación de la Voz sobre IP.
Esto no ha significado la desaparición de las redes de telefonía analógica, sino de la coexistencia de ambas redes mientras se añaden Gateways o puertas de enlace que permiten interconectar ambas tecnologías.

Más adelante, en la historia de las redes conmutadas por paquetes, se encontró oportuno la ampliación de la cobertura de las redes IP cuyo medio de transmisión sea un cable al medio inalámbrico. La motivación principal fue la libertad de movimiento, mientras que su lugar dentro de la topología fue un elemento adicional a una LAN. Así nace la familia de estándares 802.11, un conjunto de estándares con una amplia gama de innovaciones en términos de técnicas y velocidades de transmisión así como de topología, calidad de servicio y fast-roaming. En términos comerciales, desde dicho surgimiento estas tecnologías han tenido un éxito notable marcado por las 294 millones de unidades vendidas en el 2005 y un estimado de 400 millones para el 2009.

La notoria popularización de las redes inalámbricas 802.11 ha venido acompañada de una diversificación de los servicios, entre ellos, la comunicación de voz. Sin embargo, las redes inalámbricas presentan nuevos inconvenientes para la comunicación de voz en términos de la Calidad de Servicio, razón de ser de la presente tesis.

Por otra parte, el estándar inalámbrico 802.11s de Redes Inalámbricas Amalladas (Wireless Mesh), ha atraído a la investigación en gran medida gracias al ahorro sustancial práctico al eliminar en gran medida

el cableado estructurado, y al presentar nuevos retos mientras se evalúan los protocolos de enrutamiento, en la búsqueda del conjunto de procedimientos que minimicen el procesamiento del cpu y los retardos, a la vez que se maximicen la velocidad de transmisión.

Si bien es cierto, las redes 802.11 no fueron inicialmente diseñadas para la comunicación de voz en términos de diseño y en su propósito final, no obstante, también es cierto que la investigación es un motor de la innovación para presentar soluciones ante inconvenientes tecnológicos, como es el que presentan estas redes. Es por ello que la presente Tesis presenta el estudio y la prueba, mediante un Testbed, de una solución en redes Inalámbricas Amalladas (Wireless Mesh).

1.1.1. Limitaciones en las redes 802.11 tradicionales

Las redes 802.11 ofrecen movilidad a los clientes, los cuales se benefician de la conectividad sin cables permanente mientras se encuentren dentro del rango de la red completa.

El hecho de contar con una conexión directa al backhaul (o conexión al backbone principal) en cada nodo, ofrece una mayor velocidad de transmisión de datos por nodo, evitando la reducción del throughput de

la red a la mitad, como sucede con cualquier repetidor para la señal de una red 802.11 cualquiera y, por tanto, para las redes Mesh inalámbricas.

No obstante, para mantener conectividad es necesario contar con un backbone a lo largo de toda la red. Esto resulta ser muy oportuno para redes implementadas en áreas pequeñas aunque sigue siendo una desventaja por la necesidad de contar con un backbone que conecte a todos los nodos inalámbricos. Si el backbone falla, los nodos pierden conectividad. Es también necesario contar con repetidores cada 100 metros aproximadamente. Todo esto resulta en costos adicionales que, por supuesto, llega a ser una desventaja clara.

1.1.2. Limitaciones en las redes Wireless Mesh

Las Redes Wireless Mesh cuentan con una mayor autonomía respecto de las redes 802.11 tradicionales al no necesitar de mantenerse conectados en todos los nodos a un backbone que sirva de backhaul.

Sin embargo, las redes mesh inalámbricas cuentan con dos principales limitaciones: la reducción del throughput por salto y el overhead característico de las redes mesh que resulta en un exceso de tráfico en

la red. Adicionalmente, se pierde cobertura global de la red, al necesitar que los nodos se encuentren a una distancia aún menor de lo que necesitan los nodos de una red 802.11 tradicional.

1.2. Descripción del problema

Añadir movilidad a la comunicación de Voz sobre IP ha sido una fuerte motivación para la industria desde los inicio de la misma. Sin embargo, añadir movilidad tiene una limitante importante determinada por la Calidad de Servicio (QoS), un parámetro fundamental en el diseño de una red Voz sobre IP al determinar la idoneidad del sistema para soportar una cantidad determinada de llamadas concurrentes, así como los requerimientos técnicos mínimos para llevar a cabo una conversación fluida.

El principal problema radica en que las redes IP no fueron inicialmente planificadas para soportar una comunicación de Voz fluida. Debido a esto, la comunicación de voz a través de dichas redes tiene una calidad inferior a las tecnologías inicialmente diseñadas para soportar tráfico de voz. Una solución que se encontró para las redes de voz sobre IP comunes (cuyo medio físico es el cable de Ethernet) fue agregar prioridades a los paquetes, de modo que los paquetes que tienen

información de voz poseen una prioridad superior a otros que no poseen dicha clase de información. No obstante, las redes 802.11 añaden nuevos elementos que afectan de manera directa a la comunicación de voz: mayor latencia y handoffs.

Por otro lado, la necesidad de contar con movilidad dentro de un área de trabajo es esencial. La necesidad de llevar consigo un medio de comunicación móvil y utilizable en cualquier lugar dentro de un lugar de trabajo es un adelanto en términos tecnológicos.

Adicionalmente, el aspecto financiero es un factor importante al tomar una decisión sobre la mejor solución al implementar a gran escala.

Un estudio más detallado acerca de los handoffs se puede verificar en el capítulo 2.

1.3. Soluciones Disponibles

1.3.1. El Estándar 802.11r

En los primeros días de 802.11, los handoffs era una tarea mucho más simple para el cliente móvil: sólamente eran necesarios cuatro mensajes para establecer una nueva conexión a un nuevo punto de acceso (cinco

si se cuentan el mensaje opcional que el cliente envía al punto de acceso del cual está saliendo para informar que está siendo atendido por un nuevo punto de acceso). En un ambiente automotriz, esto podría significar un handoff cada 5 o 10 segundos.

Sin embargo, a medida que nuevas innovaciones se han añadido al estándar, el número de mensajes requeridos han ido en aumento dramáticamente. Durante el tiempo en el que los mensajes adicionales son intercambiados, el tráfico del móvil -incluyendo el de una llamada- no pueden proseguir y el usuario puede percibir una pérdida de información en ese tiempo. Generalmente, el retardo máximo o pérdida que la red debería introducir es de 150 milisegundos.

802.11r fue lanzado como un esfuerzo por aminorar la carga que la seguridad y la Calidad de Servicio añadieron al proceso de handoff, y restaurar el antiguo intercambio de cuatro mensajes. De esta manera, los problemas de handoffs no son eliminados, pero al menos son aminorados.

La primera aplicación actualmente prevista para este estándar es la Voz sobre IP vía teléfonos móviles diseñados para trabajar con redes inalámbricas de internet, en lugar o en añadidura a las redes celulares.

IEEE 802.11r especifica transiciones rápidas de BSS entre puntos de acceso al redefinir el protocolo de negociación "key negotiation protocol", permitiendo tanto a la negociación como los pedidos accesar a servicios inalámbricos. Dicho protocolo de 802.11i especifica que, para una autenticación basada en 802.1X, el cliente debe renegociar su "key" con el Radius u otro servidor de autenticación que soporte un Protocolo Extensible de Autenticación (EAP) en cada handoff. La solución es permitir que parte del "key" derivado del servidor sea almacenado en la red inalámbrica, de modo que un futuro número de conecciones puedan basarse en el "key" almacenado y, con ello, se evita usar el proceso 802.1X. Actualmente existe un almacenamiento llamado Opportunistic Key Caching basado en 802.11i, que realiza la misma tarea. 802.11r difiere de OKC al especificar una jerarquía completa de "keying", o almacenamiento de "keys".

1.3.2. SMesh

SMesh es un sistema mesh inalámbrico creado por el grupo de sistemas y redes distribuidas de la Universidad de Johns Hopkins. Ofrece fast-handoffs para soluciones VoIP u otras aplicaciones en tiempo real sin necesidad de modificar los clientes 802.11 tradicionales. En SMesh, la

red completa es vista por los clientes mesh como un punto de acceso omnipresente.

Los handoffs son posibles gracias a la seguridad de que cada cliente es atendido por al menos un punto de acceso en cualquier momento. Los clientes móviles son atendidos por un sólo punto de acceso durante los momentos de conectividad estables. Durante las transiciones, SMesh utiliza más de un punto de acceso para atender al cliente en movimiento. Los puntos de acceso monitorean continuamente la calidad de la conectividad de cualquier cliente dentro de su cobertura y comparten eficientemente la información con los puntos de acceso vecinos a ese cliente para coordinar cuál de ellos debería atenderlo.

Debido a que esta es una de las soluciones propuestas en la presente tesis y se encuentra incluída dentro de la hipótesis, considero necesario realizar un estudio mucho más detallado de este sistema.

Arquitectura SMesh

Se considera un conjunto de puntos de acceso 802.11 conectados en una red mesh inalámbrica y un conjunto de clientes mesh inalámbricos que pueden desplazarse dentro del área cubierta por el conjunto de

puntos de acceso. Se le llama a cada punto de acceso un nodo en la red mesh inalámbrica.

La topología mesh cambia cuando cambia la conectividad entre los puntos de acceso, cuando un nodo presenta un problema o se recupera de él, o cuando nodos adicionales son añadidos para expandir la cobertura inalámbrica. Los clientes móviles no forman parte de la topología mesh. Algunos de los nodos mesh, pero no todos, poseen una conexión cableada a Internet. A esos nodos se los conoce como puertas de enlace a Internet. Cada nodo mesh debe ser capaz de llegar a la puerta de enlace a Internet más cercana o a cualquier otro nodo a través de una secuencia de saltos.

Los clientes móviles son dispositivos 802.11 que no presentan ninguna modificación. Se comunican con los nodos mesh para accesar a la red. No se especifican controladores especiales, ni hardware o software para el cliente. Por lo tanto, cualquier cliente móvil 802.11 puede utilizar transparentemente la red mesh.

Infraestructura de Comunicaciones

Los nodos mesh crean una red Ad-Hoc inalámbrica relativamente

estable. Dentro de esta red, los nodos necesitan reenviar los paquetes a través de múltiples saltos para comunicarse con la puerta de enlace a Internet o para coordinar decisiones relacionadas a atender a los clientes móviles. Los nodos también necesitan descubrir y monitorear a sus vecinos y automáticamente ajustar el enrutamiento mesh en caso de que la topología cambie.

La infraestructura de comunicaciones de SMesh recae en un sistema de mensajería llamado Spines. La red Spines interconecta a todos los nodos a través de enlaces directos en la red inalámrbica y a través de enlaces virtuales en la red cableada. SMesh crea una instancia de Spines en cada nodo para redirigir los mensajes dentro de la red mesh inalámbrica. Cada instancia monitorea a sus vecinos directos enviando mensajes hello periódicamente. Basados en la conectividad disponible, cada nodo crea un enlace lógico inalámbrico con su vecino directo y utiliza un protocolo de estado-enlace para intercambiar información de enrutamiento con otros nodos dentro de la red.

Los nodos inundan de información de estado-enlace utilizando enlaces confiables entre los vecinos cercanos. Esto permite que los nodos envíen actualizaciones incrementales únicamente, y solamente cuando la topología de la red cambia. Las actualizaciones del estado del enlace

contienen únicamente información acerca de los enlaces inalámbricos que cambian su estado. Cuando no existen cambios en la topología, no se intercambia información de enrutamiento. Considerando que los nodos mesh (puntos de acceso) son estacionarios prácticamente todo el tiempo y que los cambios de topología son relativamente raras, el mecanismo incremental del estado-enlace produce en muy baja tasa de overhead. A pesar de que este protocolo de estado-enlace no podría ser óptimo para una red Ad-Hoc móvil, resulta ser viable para una red relativamente estable y estática como SMesh.

Dado que opera en base a software, Spines permite utilizar funcionalidades multicast y unicast en un ambiente multi-salto sin necesidad del soporte de la infraestructura. Un grupo multicast está definido en las direcciones IP multicast de clase D, mientras un grupo unicast es una dirección de clase E. Cabe mencionar que los grupos son definidos en el espacio virtual de direccionamiento de Spines y no en el espacio de direccionamiento IP de la red. Cuando un nodo se une o sale de un grupo, la instancia de Spines local informa a todos los otros nodos en la red a través de un inundación confiable similar al protocolo de estado-enlace. Solamente las entradas y salidas son inundadas a todo el sistema. La membresía al grupo es mantenida en Spines en tuplas de la forma (dirección del nodo mesh, dirección del grupo), de tal

modo que cada nodo conoce todos los grupos a los que pertenecen otros nodos.

Basados en la membresía y disponibilidad de conectividad, Spines automáticamente construye un árboles multicast a través de la red mesh. Un mensaje de dato multicast sigue el árbol multicast correspondiente a su grupo. Por lo tanto, si varios nodos en una cierta vecindad se unen a un grupo multicast, los mensajes multicast intercambiados entre ellos sólo serán enviados en esa vecindad. Un mensaje de dato anycast, por otro lado, sigue un camino único en el árbol a su miembro más cercano del grupo. Los árboles multicast en Spines son construidos optimizando una métrica que puede basarse en el número de saltos, retardo del enlace o pérdida de paquetes.

En pruebas realizadas por sus creadores, Spines pudo manejar varios cientos de miles de miembros de grupos en computadoras de escritorio y estaba limitado únicamente a la memoria disponible para mantener las estructuras de datos. Los routers Linksys WRT54G utilizados en las pruebas de la presente tesis tienen suficiente memoria como para manejar al menos 1000 clientes móviles al mismo tiempo.

Métrica de Enrutamiento

En una red mesh con múltiples puertas de enlace a Internet, las conexiones cableadas pueden ser utilizadas como atajos a comunicaciones inalámbricas que requieran de muchos saltos, decreciendo el número de transmisiones inalámbricas. Por esta razón SMesh mantiene una infraestructura híbrida con enlaces inalámbricos y cableados.

En general, en una esquema combinado de métricas de enrutamiento cableado-inalámbrico es razonable asumir que una conexión cableada tiene un costo mucho menor que un enlace inalámbrico. Por otro lado, dependiendo de las condiciones de la red es posible que las conexiones cableadas entre las puertas de enlace de Internet tengan costos diferentes (en términos de tasa de pérdidadas de paquetes, throughput, retardo, etc.).

La solución en SMesh utiliza la mejor ruta a un destino considerando la conectividad inalámbrica así como cualquier ruta híbrida disponible, y permite utilizar diferentes métricas de enrutamiento tanto en enlaces cableados e inalámbricos.

Considerando que cada enlace inalámbrico puede tener una métrica del CostoActual de al menos 1, el costo de enrutamiento de ese enlace será:

$$Costo = CostoActual * (M + 1)$$

Donde M es el costo máximo que puede ser asociado con un camino cableado.

El costo de un camino híbrido es la suma del costo de todos los enlaces. Este mecanismo da preferencia a cualquier enlace cableado sobre uno inalámbrico y optimiza el camino cableado basándose en la métrica deseada.

Interfaz con los Clientes Móviles

SMesh provee la ilusión de un solo punto de acceso omnipresente distribuido. Esto es conseguido al proveer la información de conectividad a los clientes a través de DHCP y al dar siempre la misma información (Dirección IP, Máscara y puerta de enlace predeterminada) al cliente móvil.

Conectividad con los Clientes Móviles

Cada nodo mesh ejecuta un servidor DHCP que está a cargo de proveer información de inicio de la red, incluyendo una dirección IP única, a un cliente determinado. Se computa esa dirección IP utilizando una función hash en la dirección MAC del cliente, mapeado a una dirección privada de clase A de la forma 10.A.B.C.

Una porción pequeña de la dirección IP privada en este rango es reservada para los nodos SMesh y el resto se encuentra disponible para los clientes móviles. En el caso de una colisión hash, el cliente con la dirección MAC menor mantiene su dirección IP y cualquier otro cliente en la colisión obtiene una dirección IP mediante IPAM (servicio de DHCP). Este esquema decrementa el número de direcciones IP entregadas utilizando IPAM mientras se asegura que cada cliente obtenga la misma dirección IP de cualquier nodo SMesh.

Los elementos de importancia en DHCP son: el ID de Servidor, la Puerta de Enlace Predeterminada y los lease timers (temporizador de alquiler) T1 y T2. La puerta de enlace predeterminada especifica el siguiente salto a utilizar a nivel MAC cuando se envía a una dirección IP fuera de la máscara de red del cliente. El ID del Servidor especifica la dirección

IP del Servidor de DHCP que el cliente puede contactar para renovar su tiempo de alquiler (tiempo en el cual debe reportar el uso de su conectividad).

Los temporizadores T1 y T2 especifican cuándo empezar los pedidos DHCP unicast o broadcast, y el temporizador de alquiler especifica cuándo debe el cliente dejar de utilizar la dirección IP que tiene. Luego de que el temporizador expira, todas las conexiones con el cliente son terminadas. Si el punto de acceso responde a un pedido DHCP antes de que el temporizador expire, puede mantener las conexiones abiertas. En SMesh, el temporizador está fijado en 90 segundos, lo cual le da el tiempo suficiente al cliente para reconectarse en caso de que se salga de la cobertura de cualquiera de los nodos mesh temporalmente.

En cuanto al esquema de direccionamiento, se le asigna una pequeña subred a cada cliente, forzando así al cliente a enviar paquetes destinado ya sea a Internet o a otro punto vía su puerta de enlace predeterminada. La dirección IP de la puerta de enlace predeterminada es virtual; no existe ningún nodo en SMesh con esa dirección IP. En su lugar, SMesh le hace "creer" al cliente que esta dirección es alcanzable al asociar esta dirección IP a la dirección de hardware de un nodo mesh.

Esto obliga al cliente a enrutar los paquetes a través de un punto de acceso SMesh.

Mientras que cada cliente en SMesh consume 3 bits del espacio de direccionamiento, existen aún 21 bits disponibles, lo cual permite manejar hasta un millón de direcciones IP.

Grupos SMesh

Los nodos mesh sirven como puertas de enlace predeterminadas para los clientes móviles. Un módulo de paquetes proxy utiliza un interceptor para recolectar paquetes enviados por un cliente y una interfaz para reenviar los paquetes de vuelta al cliente.

Cada cliente móvil está asociado a un grupo multicast único en la red mesh: el grupo de datos, para que los puntos de acceso reciban los datos del cliente. Uno o más nodos mesh que se encuentran en la vecindad de un cliente se unirán al grupo de datos del cliente.

Si el destino de un paquete es un cliente SMesh, el paquete es enviado a los nodos SMesh que se han unido al grupo de datos del cliente. El nodo SMesh que envía este paquete puede ser la puerta de enlace de

Internet (para paquetes que vienen de Internet) o un punto de acceso del cliente que envía dicho paquete. Al recibir un paquete de un cliente, cada uno de los nodos que se unieron al grupo de datos de ese cliente reenvía el paquete al cliente. Si el destino del paquete es Internet, entronces el paquete es enviado por el punto de acceso del cliente que origina el paquetel. Debido a que los clientes se manejan en un entorno de direcciones privadas, las puertas de enlace a Internet ejecutan NAT antes de reenviar el paquete al internet. Cuando un paquete respuesta es recibido del Internet, se realiza un proceso NAT inverso. Bajo circunstancias normales, sólamente un nodo se une a este grupo. Spines reenvía los paquetes a los miembros del grupo de datos del cliente utilizando un árbol multicast. De esta manera, si el cliente móvil se ha movido, y un nodo SMesh diferente se une al grupo de datos del cliente, los paquetes son reenviados al nuevo nodo SMesh en el grupo. Los nodos SMesh en el grupo de datos del cliente utilizan un socket para enviar los paquetes, permitiendo al cliente recibir los paqutes como si se hubiese conectado directamente con el host de destino. Si existen múltiples nodos en el grupo de datos, el cliente podría recibir paquetes IP duplicados. Sin embargo, los paquetes IP duplicados son descartados a nivel de TCP en el receptor.

En adición al grupo de datos del cliente utilizado para reenviar los paquetes de datos en SMesh a los puntos de acceso atendiendo al cliente, los puntos de acceso en la vecindad del cliente se unen a un grupo multicast diferente específico a ese cliente, llamado el grupo de control. El grupo de control del cliente es utilizado para coordinar con otros nodos mesh en la vecindad del cliente con respecto a las métricas de la calidad del enlace y a cuál es el mejor punto de acceso en atender a ese cliente. Un nodo mesh se une a un grupo de control del cliente cuando escucha paquetes provenientes del cliente, y deja el grupo cuando deja de escuchar dichos paquetes por algún tiempo. Los nombres de tanto el grupo de control como el grupo de datos son derivados de la dirección IP del cliente: para un cliente cuya dirección es 10.A.B.C, un nodo SMesh se unirá al grupo de control del cliente en 224.A.B.C y, de ser necesario, al grupo de datos del cliente en 225.A.B.C. Esto mapea a cada cliente a un conjunto de dos grupos multicast únicos.

Protocolo Intra-Dominio de Handoff

Debido a que los dispositivos 802.11 están configurados en modo infraestructura (BSS), realizan sus propios escaneos en búsqueda de el mejor punto de acceso disponible. Un handoff en capa 2 es posible a

través de un proceso de pedido/respuesta de reasociación que puede durar algunos segundos. En adición, durante estos handoffs el cliente puede hablar únicamente con uno de los puntos de acceso al mismo tiempo y el cliente no puede comunicarse con el antiguo punto de acceso durante el proceso.

Para evitar este comportamiento y controlar los handoffs únicamente por los puntos de acceso, se configura tanto los puntos de acceso como los clientes móviles en modo Ad-Hoc (IBSS). Una manera de realizar los handoffs en modo Ad-Hoc es mediante el protocolo DHCP. Por ejemplo, uno puede instruir al cliente de renovar su alquiler de IP cada cierto tiempo. Cualquier punto de acceso que escuche el pedido DHCP puede responder y convertirse la puerta de enlace predeterminada. Mientras que este mecanismo puede proveer de cierta capacidad de handoff, el proceso puede demorar varios segundos debido a que el nodo necesita esperar a que el cliente inicie la transacción DHCP. Además, el cliente puede conectarse a través de un punto de acceso que tiene una conexión débil, mientras que podría conectarse con otros nodos con mejores niveles de potencia.

En lugar de permitir que el cliente "decida" cuándo realizar el handoff, los nodos SMesh mantienen un seguimiento de la conectividad de sus

clientes y los inducen a cambiar su punto de acceso donde haya una mejor conectividad. Para conseguir esto sin modificar al cliente, se provee la ilusión de una puerta de enlace predeterminada fija y se utilizan mensajes ARP para obligar a efectuar la transición al nodo SMesh con la mejor conectividad para el cliente.

Para mantener la conectividad con el cliente, se emplea la estrategia de utilizar DHCP y ARP. Cuando se utilizar el Monitor DHCP SMesh, el servidor DHCP instruye a los clientes renovar su dirección IP cada 2 segundos, de esta manera sirve como un monitor constante que sigue los movimientos del cliente. Un punto bajo es que emplea un overhead como un paquete DHCPREQUEST de 300 bytes, y un DHCPACK tiene alrededor de 548 bytes. Otro punto bajo es que, si el primero DHCPREQUEST se pierde, el tiempo entre su pedido y el siguiente depende de la plataforma y usualmente toma algunos segundos.

El protocolo ARP, por otro lado, es utilizado para mapear las direcciones IP a direcciones de hardware (MAC), cuando un host desea comunicarse con otro dentro de la misma red. SMesh envía regularmente paquetes gratuito ARP para que el cliente envíe respuestas ARP unicast o broadcast. Se instruye al cliente de enviar su respuesta a una dirección IP especial dentro de su subred, con una

dirección MAC de los puntos de acceso que enviaron la respuesta (por ejemplo, un paquete enviado por el AP 10.0.0.31 al cliente 10.11.12.25 es un paquete ARP "Quién tiene 10.11.12.25?, díle a 10.11.12.27", donde la dirección MAC asociada con 10.11.12.27 es realmente la MAC de 10.0.0.31). Esto es necesario debido a que la dirección IP real de SMesh se encuentra fuera de la red del cliente. La ventaja de utilizar esta solución es que, a diferencia de DHCP, los paquetes ARP son muy pequeños (28 bytes). En SMesh, se requieren respuestas ARP de los clientes cada uno o dos segundos. Además, se limitan el número de puntos de acceso que se comunican con el cliente, sólamente el nodo Mesh dentro del grupo de datos del cliente envía pedidos periódicamente, y todos los nodos en la vecindad utilizan esta respueta para computarizar la métrica.

Handoffs de los Clientes

Cada nodo mesh tiene una dirección IP que le permite comunicarse con otros nodos mesh. Sin embargo, para proveer un handoff transparente a los clientes, los nodos mesh muestran una puerta de enlace predeterminada virtual a todos los clientes con sus respectivas ofertas DHCP y ACKs (DHCPOFFER y DHCPACK). Los clientes móviles fijan su puerta de enlace predeterminada a dicha dirección IP virtual sin

importar a cuál punto de acceso se encuentran conectado. De esta forma, los clientes móviles tienen la ilusión de estar conectado a un sólo punto de acceso que lo sigue mientras se mueven. La dirección IP de la puerta de enlace predeterminada sólamente aparece en la oferta DHCP. En todas las demás comunicaciones con los clientes móviles, la puerta de enlace predeterminada no aparece en los paquetes IP.

La dirección IP puede ser fijada a cualquier dirección IP de la subred a la que pertenece el cliente dado que la comunicación con los clientes móviles se basa únicamente en direcciones MAC. El mecanismo de handoff utiliza mensajes ARP para cambiar instantáneamente el punto de acceso utilizado por el cliente. Un paquete gratuito ARP es un paquete respuesta ARP que no es enviado como una respuesta a una petición ARP, sino que es enviado voluntariamente por la red local. Típicamente, los paquetes ARP gratuitos son utilizados por los hosts para mostrar sus nuevas direcciones de hardware cuando la tarjeta de red ha sido cambiada.

Cuando un nodo SMesh considera que tiene una mejor conectividad con el cliente y decide atender a ese cliente, le envía un mensaje ARP gratuito como unicast, directamente al cliente, cambiando de esa manera su dirección MAC de puerta de enlace predeterminada.

Paquetes subsecuentes enviados por el cliente serán enviados al nuevo punto de acceso, siguiendo la nueva dirección de hardware. Adicionalmente al envío de mensajes ARP gratuitos a los clientes móviles, cuando un nodo considera que tiene la mejor calidad de enlace con un cliente móvil, se añade al grupo de datos de tal manera que los paquetes destinados al cliente empiezan a fluir desde ese punto de acceso. Si otro nodo es también parte de ese grupo de datos, los paquetes destinados a este cliente es reenviado a ambos nodos mesh, y cada uno de ellos reenvía los paquetes directamente al cliente móvil. El cliente móvil puede recibir paquetes duplicados en ese momento. Utilizar multicast ayuda a evitar interrupciones en la conectividad durante el handoff mediante: 1) el envío de paquetes a través de múltiples puntos de acceso al cliente móvil, contra los casos en los que el cliente se desplaza inesperadamente mientras se elige el mejor punto de acceso, y 2) evitando pérdidas mientras se cambia la ruta en la red mesh inalámbrica.

Un nodo mesh que se une al grupo de datos de un cliente inmediatamente envía una actualización de métrica al grupo de control para informar a cualquier nodo de su última métrica, denotando que ahora él es miembro del grupo de datos del cliente. Cuando un nodo mesh que es parte de un grupo de datos recibe una actualización de

métrica de calidad de enlace que muestra que un nodo diferente en el grupo de datos tiene una mejor conexión, envía un pedido de salida. Los pedidos de salidas enviados al grupo de control, son enviados con piggy-backing en las actualizaciones de métricas de calidad del enlace. Un pedido de salida puede ser aceptado (ACK) por un nodo en el grupo de datos que considera que tiene la mejor conectividad con el cliente. Un nodo puede salir del grupo de datos si y sólo si su pedido es aceptado (ACK) por al menos otro nodo.

1.3.3. Otras Soluciones

Meraki

Meraki es una compañía que provee de hardware y software de redes inalámbricas. Utiliza un sistema de control centralizado en los servidores de la compañía. Fue fundada por dos estudiantes de PhD de Stanford basados en su proyecto de roofnet.

El software de manejo de Meraki (llamado "dashboard") le permite a la red configurarse y ajustarse vía web. En el mapa que provee Meraki es posible identificarlos por etiquetas. Identifica automáticamente el entorno y elabora estadísticas. Existen características de software que

gobiernan tanto el ancho de banda consumida por el tráfico de la parte inalámbrica así como formas de optimizar el uso del ancho de banda. Las operaciones de la central de Meraki juegan una parte en ayudar a balancear las cargas de la red entre los diferentes nodos y reportar en el estatus global de la situación de los nodos y de la red en general.

Enrutamiento con Meraki

Meraki utiliza enrutamiento Mesh. El firmware utiliza el algoritmo SrcRR (Roofnet) para determinar las rutas entre los dispositivos de hardware. El acceso al medio y el Transporte puede ser manejado por el algoritmo ExOR. Cada dispositivo envía peticiones broadcast periódicamente y los demás dispositivos en rango reportan sus rutas. Los dispositivos utilizan esa información para enrutar los paquetes a la puerta de enlace más cercana. El enrutamiento se lleva a cabo principalmente para determinar una ruta a la puerta de enlace más cercana (o dispositivo con una conexión a internet).

Cuando un nodo incializa, prueba la conectividad a internet por el puerto de internet. Si tiene conectividad con internet, se autodenomina "puerta de enlace a Internet" y se prepara a ceptar paquetes de repetidores (nodos) cercanos. Si otros nodos se encuentran en el rango y los

puertos de ethernet no están conectados, el nodo actúa simplemente como repetidor para extender la red. Meraki asegura que sólamente uno de sus repetidores necesita estar conectado a Internet para que el diseño funcione correctamente. Luego busca otros nodos Meraki y les informa de su existencia.

Roofnet es una red mesh experimental actualmente bajo desarrollo en el Laboratorio de Ciencias Computacionales y Artificiales del Instituto de Tecnología de Massachusetts. Parte del proyecto investigativo incluye mediciones a nivel de enlace de 802.11, algoritmos de búsqueda y corrección, adaptación del enlace y el desarrollo de protocolos que tomen ventaja de las propiedades únicas del radio (ExOR).

El protocolo de enrutamiento se llama SrcRR. Existen dos tipos de broadcasts utilizados en el protocolo. El primero es un broadcast periódico utilizado para determinar una métrica llamada ETX. Estos broadcasts públicos miden la probabilidad de que un paquete entre dos nodos en contacto inalámbrico llegue a su destino. El segundo broadcast es utilizado para armar tablas de enrutamiento. Un nodo A determinado envía un broadcast para encontrar la ruta a D. Entonces el nodo que recibe el broadcast añade su ID a las tablas de enrutamiento. Cuando el nodo D recibe el paquete, responderá a través de la ruta que

fue encontró el paquete. Entonces el nodo A utiliza esta información para determinar la mejor ruta utilizando las métricas ETX y la información de la ruta retornante de su petición.

El protocolo de acceso al medio y reenvío probado en RoofNet es ExOR. ExOR simula algunas de las ventajas de enviar datos multicast utilizando radios 802.11 en modo broadcast.

El nodo utiliza datos en enrutamiento establecidos en una list de radios que pueden ayudar a llegar al nodo destino. La lista es ordenada de tal forma que los nodos cercanos al de destino se encuentran más cerca al tope de la lista. El destino se encuentra al tope de la lista. La lista es almacenada de forma compacta en cada paquete. Cada paquete también incluye una lista que muestra el progreso de cada paquete a través de la lista de nodos. Esta lista tiene una entrada por paquete. Cada entrada es un número de nodos que se encuentran más cerca del destino y ha retransmitido el paquete. La importancia de la lista radica en encontrar el mejor camino en base al tiempo de recorrido y estimados probabilísticos del tiempo de retransmitir los paquetes que retransmiten los nodos cercanos al destino.

1.4. Planteamiento de Hipótesis

La Calidad de Servicio en Voz sobre Redes Inalámbricas se ve mejorada con el uso de SMesh en comparación con el uso de otras redes tradicionales Wireless Mesh y Wireless LAN tradicionales dentro de instalaciones de la FIEC.

1.5. Metodología

Para hacer efectivo el estudio de Calidad de Servicio, es necesario contar con datos objetivos y subjetivos sobre la Red de prueba. Dichos datos proveen información acerca del grado de satisfacción del usuario al utilizar la red.

Las pruebas ser realizarán dentro de las instalaciones de la FIEC en la zona del antiguo laboratorio de Telecomunicaciones. Se utilizará un software que mide Calidad de Servicio que captura los paquetes RTP que se envíen y reciban desde una laptop con un softphone registrado en una PBX Open Source. Adicionalmente, se cuenta con teléfonos celulares con capacidades VoIP en WLAN y teléonos IP convencionales Ethernet.

Se probarán tres soluciones: SMesh, Meraki y la Red Inalámbrica ESPOL por separado. Se realizarán stress tests de una llamada para poner al límite el desempeño de las redes. Los resultados arrojados serán comparados, tanto los subjetivos como los objetivos.

Los datos objetivos son proporcionados por la herramienta de trabajo WireShark, que provee datos relacionados a Calidad de Servicio, tales como jitter, delay y ancho de banda luego de una llamada. Dichos datos proveen de información necesaria para evaluar la calidad de la comunicación, en términos técnicos.

Los datos subjetivos serán dados por el MOS (Mean Opinion Score), que es un método tanto subjetivo como objetivo relacionado que mide el grado de satisfacción del usuario en una escala del 1 al 5. Para el caso de la presente tesis, esos valores serán calculados utilizando el modelo E modificado que incluye los valores de Jitter de la red.

CAPÍTULO 2

2. FUNDAMENTOS DE VOZ SOBRE IP SOBRE WLANS Y CALIDAD DE SERVICIO

Para realizar un estudio de las condiciones de la comunicación de voz sobre redes 802.11 en general, es necesario primero realizar un recorrido por los conceptos más reelevantes relacionados tanto a las redes 802.11 como a la voz sobre IP en redes 802.11 y la Calidad de Servicio (QoS).

2.1. Las Redes Wireless LAN 802.11

2.1.1. La familia de estándares 802.11

En términos generales, el estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (física y enlace de datos), especificando sus normas de funcionamiento en una WLAN. La familia

de estándares IEEE 802.11 incluye técnicas de modulación que usan el mismo protocolo básico. Durante el tiempo, los estándares más popularizados fueron el estándar 802.11b y 802.11g, que son versiones cambiadas del primer estándar de redes inalámbricas, 802.11-1997. En la presente sección se detallan los estándares más importantes para el estudio de la presente tesis.

IEEE 802.11a: Fue aceptado en 1999 como una modificación del primer estándar original. Utiliza el mismo protocolo, mientras que opera en la banda de 5 Ghz, utilizando 52 sub-portadoras OFDM con una máxima tasa de datos ideal de 54 Mbit/s y una tasa de datos real de 20 Mbit/s. Originalmente tuvo 12/13 canales que no causaban interferencia entre ellos. Este estándar no es interoperable con 802.11b ni 802.11g, debido que operan en bandas diferentes, excepto que se utilicen equipos con capacidad de banda dual.

Utilizar la banda de 5 Ghz le da una ventaja significativa a 802.11a, debido a que la banda 2.4 Ghz está actualmente saturada por la cantidad de dispositivos que la utilizan (desde la popularización de la banda 2.4 Ghz como banda no licenciada). Sin embargo, el uso de una portadora con frecuencias elevadas produce una reducción sustancial en la cobertura por punto de acceso.

IEEE 802.11b: Tiene una tasa de datos máxima de 11 Mbit/s y utiliza el mismo método CSMA/CA definida en el estándar original. Debido a la cabecera del protocolo, en la práctica el máximo throughput que una aplicación 802.11b puede alcanzar es alrededor de 5.9 Mbit/s utilizando TCP y 7.1 Mbit/s utilizando UDP. Debido a que 802.11b es una extensión directa de la técnica de modulación DSSS definida en el estándar original. No obstante, debido a que trabaja en la banda de 2.4 Ghz, sufre de interferencias con dispositivos como: microondas, dispositivos bluetooth, monitores para bebés y teléfonos inalámbricos.

IEEE 802.11g: Fue el tercer estándar de modulación para Redes Inalámbricas de Área Local. Trabaja en la banda de 2.4 Ghz, pero opera a una tasa de datos máxima ideal de 54 Mbit/s, o a cerca de 19 Mbit/s flujo neto. Los equipos de este estándar son compatibles con el estándar 802.11b. A pesar de que los esfuerzos de diseño de hardware han permitido que coexistan ambas tecnologías en un mismo equipo, la participación de 802.11b en la red bajo el mismo equipo reduce la velocidad de la red 802.11b. El esquema de modulación utilizado e 802.11g es OFDM, al igual que 802.11a.

IEEE 802.11s: Es una enmienda del estándar IEEE 802.11 en fase aún

de revisión para las redes Inalámbricas Amalladas (Wireless Mesh Networks). Define cómo los equipos pueden interconectarse para crear una red ad-hoc. Gracias a ello, puede funcionar en cualquiera de los sub estándares 802.11a/b/g/n. Extiende el estándar MAC IEEE 802.11 definiendo una arquitectura y un protocolo que soportan tanto broadcast como multicast y unicast enviando "métricas de radio sobre toplogías de saltos múltiples auto configurables".

En dispositivo Wireless Mesh se lo conoce como Mesh Station (mesh STA). Dichos mesh STAs forman vínculos uno con otro, sobre el cual se pueden estabelcer caminos utilizando un protocolo de enrutamiento. 802.11s define un protocolo de enrutamiento predeterminado llamado HWMP (Hybrid Wireless Mesh Protocol), aunque permite a los fabricantes crear dispositivos con protocolos propietarios. HWMP es una combinación de AODV y enrutamiento de árbol. 802.11s también incluye mecanismos que proveen acceso a la red, control de congestión y ahorro de energía.

IEEE 802.11r: es una enmienda al estándar IEEE 802.11 original para permitir conectividad continua para dispositivos inalámbricos en movimiento con handoffs seguros y rápidos de un punto de acceso a otro. Fue publicado en Julio 15 del 2008. Los handoffs, no obstante, son

actualmente manejados en los estándares existentes. La arquitectura fundamental de los handoffs 802.11 sin 802.11r es idéntica: el dispositivo móvil está en la potestad de decidir cuándo llevar a cabo el handoff y a cuál punto de acceso. 802.11r fue lanzado como un esfuerzo por aminorar la carga que la seguridad y la Calidad de Servicio añadieron al proceso de handoff, y restaurar el antiguo intercambio de cuatro mensajes. De esta manera, los problemas de handoffs no son eliminados, pero al menos son aminorados.

2.1.2. Arquitectura

Una red 802.11 está basada en una arquitectura celular donde el sistema es subdividido en celdas. Una red IEEE 802.11 es comunmente una extensión inalámbrica dentro de una red de área local, aunque es posible prescindir de una LAN convencional para conformar una red WLAN 802.11.

Los elementos básicos de una WLAN son las estaciones y los puntos de acceso. Las estaciones son los clientes como laptops, PDAs o teléfonos móviles, mientras que los puntos de acceso pueden bien ser enrutadores o repetidores inalámbricos. Para formar una WLAN, es necesario que dos de los elementos mencionados se comuniquen.

Cuando una o más estaciones se conectan a un punto de acceso, dicho conjunto se conoce como BSS (Basic Service Set, o Conjunto Básico de Servicio). En este punto, los dispositivos intercambian paquetes por el medio inalámbrico. El estándar 802.11 utiliza al BSS como un bloque genérico básico de red. A la cobertura del BSS determinada por las características transmitivas del punto de acceso se la denomina BSA (Basic Service Area, o Área de Servicio Básico).

Un SSID es un nombre que identifica a una WLAN en particular. Un cliente (o estación) recibe los SSID de todos los puntos de acceso que formen parte de una WLAN diferente. Un SSID está definida como una secuencia de 1-32 octetos, cada uno de los cuales puede tomar un valor cualquiera.

Es posible también agrupar estaciones sin conectarse a un punto de acceso, a dicho conjunto en comunicación se lo llama IBSS (Independent BSS, o BSS Independiente). A este tipo de redes inalámbricas se las conocen como redes Ad-Hoc, cuyo término proviene de una locución latina que hace referencia a una solución elaborada para un problema en específico.

Cuando uno o más BSSs se unen bajo un mismo SSID, al conjunto se

lo conoce como ESS (Extended Service Set, o Conjunto Extendido de Servicios). Un DS o Sistema de Distribución, es el medio por el cual los puntos de acceso se comunican de manera directa. Normalmente es el backbone que está funcionando de enlace entre la WLAN y la LAN de la cual se extiende.

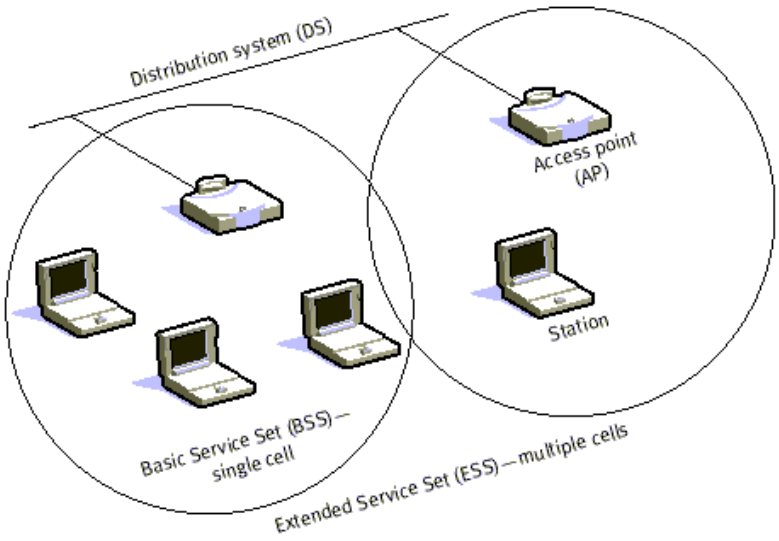

Figura 2-1. Arquitectura general de una Red 802.11

Como se mencionó anteriormente, uno de los requerimientos de IEEE 802.11 es que puede ser utilizado con una red cableada. Para solucionar esto, se utilizan Portales. Un portal es la integración lógica entre una LAN y una WLAN 802.11. Esto puede también servir como un punto de acceso a un DS. Todos los datos que van a una LAN 802.11

desde una LAN 802.X deben pasar a través de un Portal. De esta manera funciona como un puente entre lo cableado y lo inalámbrico.

Aunque que la implementación de un DS no está especificada, 802.11 sí especifica los servicios que el DS debe ofrecer. Dicho servicios esán divididos en dos: Servicios de Estación (SS) y Servicios de Sistemas de Distribución (DSS).

Los Serivicios de Sistemas de Distribución incluyen: Asociación, Reasociación, Desvinculación, Distribución e Integración. Los tres primeros están relacionados con la movilidad. Si una estación dentro de su propio BSS está ya sea en movimiento o en ausencia de él, el estado de la estación se conoce como de "no transición". Si una estación se mueve entre BSSs dentro del mismo ESS, su movilidad está determinada como una transición BSS. Si la estación se desplaza entre BSSs de diferentes ESS, su movilidad está determinada como de transición ESS. Una estación debe afiliarse con la infraestructura BSS si desea utilizar la LAN. Esto es posible Asociándose a un punto de acceso. Las aosicaciones son de naturaleza dinámica debido a que las estaciones se desplazan, se encienden o apagan. Una estación solo puede estar asociada con un punto de acceso. Esto asegura que el DS siempre está en pleno conocimiento de la ubicación de la estación.

La asociación permite una movilidad de no-transición pero no es suficiente para manejar una transición BSS. Para ello está la Reasociación, este servicio permite que la estación cambie su estado de asociación de un punto de acceso a otro. Ambas asociaciones y reasociaciones son iniciadas por la estación. La desvinculación se produce cuando la asociación entre una estación y el punto de acceso es terminada. Esto puede ser iniciado por cualquiera de las dos partes. Una estación desvinculada no puede enviar o recibir datos. No obstante, la transición entre ESS no está soportada, por lo que una estación que se desplaza entre ESS debe reiniciar conexiones.

La Distribución es simplemente tomar los datos desde el emisor a un receptor deseado. El mensaje es enviado al punto de acceso local de entrada y luego distribuido a través del DS al punto de acceso de salida al cual se encuentra asociado el receptor. Si el emisor y el receptor se encuentran dentro de la misma BSS, el punto de acceso de entrada y salida son el mismo. De este modo, el servicio de distribución es lógicamente invocado aunque el DS sea o no invocado. La Integración se lleva a cabo cuando el punto de acceso es un Portal. Así, las LANs 802.X se encuentran integradas en el DS 802.11.

Los Servicios de la Estación son: Autenticación, De-Autenticación, Privacidad, Envío de MSDU (Unidad de Dato del Servicio MAC). Con un sistema inalámbrico, el medio no está exactamente delimitado como en el caso de un sistema cableado. Para llevar el control de acceso a la red, las estaciones deben primero establecer su identidad.

Una vez que una estación es Autenticada, puede asociarse. La relación de Autenticación puede ser entre dos estaciones dentro de una IBSS o de un punto de acceso a una estación dentro de una BSS. La Autenticación fuera de una BSS no está soportada.

Existen dos tipos de Servicios de Autenticación ofrecidos por 802.11. El primero es el Sistema Abierto de Autenticación. Con él, cualquiera puede Autenticarse con una petición simple. El segundo tipo es Autenticación "Shared Key", con el cual es necesario que los usuarios tengan el conocimiento de un "key" secreto. Este "key" es implementado con el uso de un algoritmo privado llamado Wired Equivalent Privacy (WEP). Este "key" secreto es enviado a todas las estaciones utilizando un método seguro.

La De-Autenticación se lleva a cabo cuando cualquiera de las partes

desean terminar la Autenticación. Cuando esto ocurre, la estación es automáticamente desvinculada. Básicamente la privacidad es un algoritmo de encriptación utilizado de tal forma que otros usuarios 802.11 no puedan adentrarse al tráfico LAN de la estación. IEEE 802.11 especifica el algoritmo WEP como un método opcional para satisfacer la privacidad. A los datos que no son encriptados se los conoce como "plaintext" o "texto plano", mientras que los datos enviados con un encriptación se los conocen como "ciphertext" o "texto cifrado". Todas las estaciones inician en un estado no encriptado hasta que son Autenticadas. El envío de MSDU se asegura que la información del Servicio MAC Data Unit Service sea transferido entre los puntos de acceso. La privacidad está relacionada a la presencia o ausencia de encriptación. Wired Equivalent Privacy es utilizada para proteger a las estaciones autorizadas de los observadores de tráfico.

2.1.3. Evolución

El primer estándar 802.11 para WLANs

El Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) desarrolló el estándar IEEE 802.11 en Junio de 1997. El estándar define las capas Física y MAC de una red de área local inalámbrica. El estándar original

fue publicado como IEEE Std. 892.11-1997 y revisado en 1999, para ser publicado nuevamente como IEEE Std. 802.11-1999 (R2003).

La radio de una WLAN 802.11 operaba en la banda no licenciada de 2.4 Ghz (2.4 a 2.483 Ghz). La transimisón isotrópica máxima aceptada por la FCC (Ente regulador del uso del espectro en EEUU) en esta banda es de 1 W, pero los dispositivos 802.11 son usualmente limitados a 100 mW.

La capa física en 802.11 se divide en el Protocolo de Convergencia de Capa Física (PLCP) y la capa Dependiente de Medio Físico (PMD). El PLCP prepara/parsea las unidades de datos transmitidas/recibidas utilizando varias técnicas de acceso al medio. El PMD efectúa la transmisión y recepción de datos y la modulación/demodulación directamente accesando al medio bajo la guía del PLCP. La capa MAC 802.11 es afectada por la naturaleza del medio.

La IEEE define tecnologías 802.11 en la capa PHY y sub capa MAC de la capa de Enlace de Datos. La capa física describió tres técnicas de intercambio de datos: Infrarrojo, DSSS (Espectro Ensanchado por Secuencia Directa) y FHSS (Espectro Ensanchado por Salto de

Frecuencia).

El Salto de Frecuencia se refiere a la tecnología de Salto de Frecuencias patentada durante la segunda guerra mundial. Fue la primera evolución a DSSS y otras técnicas de transmisión más complejas. La idea es transmitir en una frecuencia determinada por un tiempo muy corto y cambiar a otra frecuencia de acuerdo a un patrón de saltos que conoce tanto el receptor como el emisor. Esto permite enfrentear problemas de interferencia de banda angosta con señales de alta potencia así como permitir la coexistencia de dos transmisores FHSSS cercanos.

Los saltos de frecuencia separan la banda ISM de 2.4 GHz en canales espaciados por 1 Mhz. El transmisor debe cambiar los canales al menos 2.5 veces por segundo (cada 400 ms o menos). Los patrones de saltos son descritos como 3 conjuntos que contienen 26 secuencias de saltos cada uno. Los conjuntos son definidos de tal manera que la interferencia mutua entre dos puntos de acceso cercanos.

La técnica de Espectro Ensanchado por Secuencia Directa es una de las técnicas más frecuentemente utilizadas y la más sencilla de implementar. Las tarjetas DSSS 802.11 son conocidas como dispositivos

de cláusula 15. Las tarjetas DSSS 802.11 pueden transmitir en canales subdivididos del rango de 2.4 a 2.4835 Ghz correspondiente a la banda ISM. La IEEE es un poco más restrictiva con las tarjetas FHSS, las cuales son permitidas de transmitir en sub portadoras de 1 Mhz de 2.402 a 2.480 GHz de la banda ISM de 2.4 Ghz.

La idea principal en DSSS es multiplicar los datos que se transmiten por una secuencia binaria pseudo aleatoria con una tasa de bits mayor.

La secuencia binaria pseudo aleatoria (PRN o PN) es llamada "secuencia de chips" y la tasa de datos de la secuencia es llamada "tasa de chips". Los datos no pueden ser recuperados a menos que se conozca la secuencia de chips.

802.11b

En 1998, Lucent Technologies y Harris Semiconductor (luego Intersil) propusieron un estándar llamado Complementary Code Keying (CCK) para alcanzar tasas de transmisión 5.5 Mbps y 11 Mbps. La IEEE adoptó CCK y lanzó el estándar 802.11b en 1999. El estándar incluía una nueva opción de transmitir cabeceras PLCP con un preámbulo pequeño de 56 bits. En el modo preámbulo tanto los delimitadores de Sincronización y

de Inicio son transmitidos a 1 Mbps. El resto de la cabecera PLCP es transmitida a 2 Mbps (utilizando DSSS DQPSK). 802.11b también introdujo el mecanismo "auto fallback rate" que no se implementó en el 802.11 original, así se estandarizó los procedimientos del ajuste de la tasa de transmisión de datos dependiendo de la calidad del enlace.

802.11a

802.11a popularizó a OFDM, una técnica de modulación antigua, a los estándares IEEE 802.11. Además de proponer una nueva ténica de modulación, 802.11a también cambia la banda ISM 2.4 GHz a la banda ISM 5 GHz. No obstante, esta banda no es continua y se divide en dos áreas: de 5.15 GHz a 5.35 GHz y de 5.725 GHz a 5.825 GHz. Ambas áreas estaban separadas por 802.11a en 12 portadoras sobrelapadas (similares a los canales 802.11) espaciadas a 20 Mhz.

Cada portadora se separa en 52 sub portadoras posicionadas de acuerdo a la Figura 2.1. Cuatro de las sub portadoras son llamadas pilotos y deben transmitir una secuencia que puede ser utilizada por el receptor para un control de sincronización.

Las sub portadoras de las señales OFDM son moduladas de tal manera

que, aunque los canales adyacentes se sobrelapan, no interfieren uno con el otro.

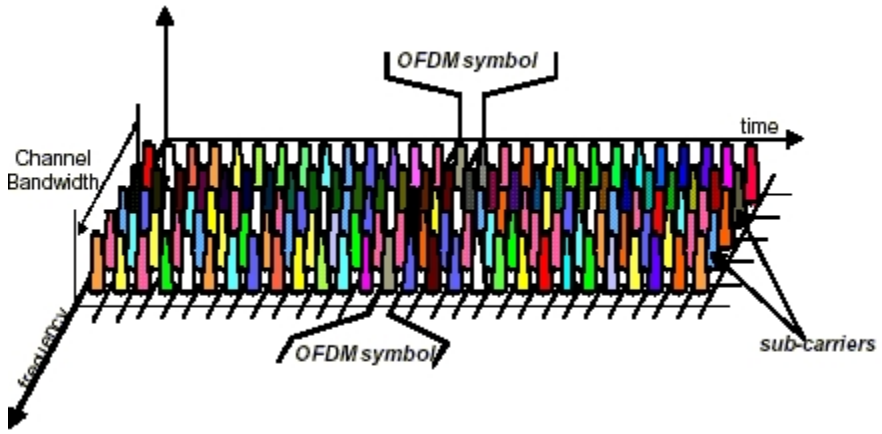

Figura 2-2 - Sub portadoras OFDM.

802.11g

A pesar de que la banda 5 GHz no está tan saturada como la de 2.4 GHz, existe un decrecimiento en el rango operacional cuando se actualiza de 802.11b a 802.11a. Además del inconveniente de cambiar todos los equipos de la red. El estándar 802.11g es la solución a estos problemas. El estándar es compatible con 802.11b y 802.11. El soporte para la modulación antigua es mandatoria. Para tasas de datos altas introduce OFDM a la banda ISM de 2.4 Ghz.

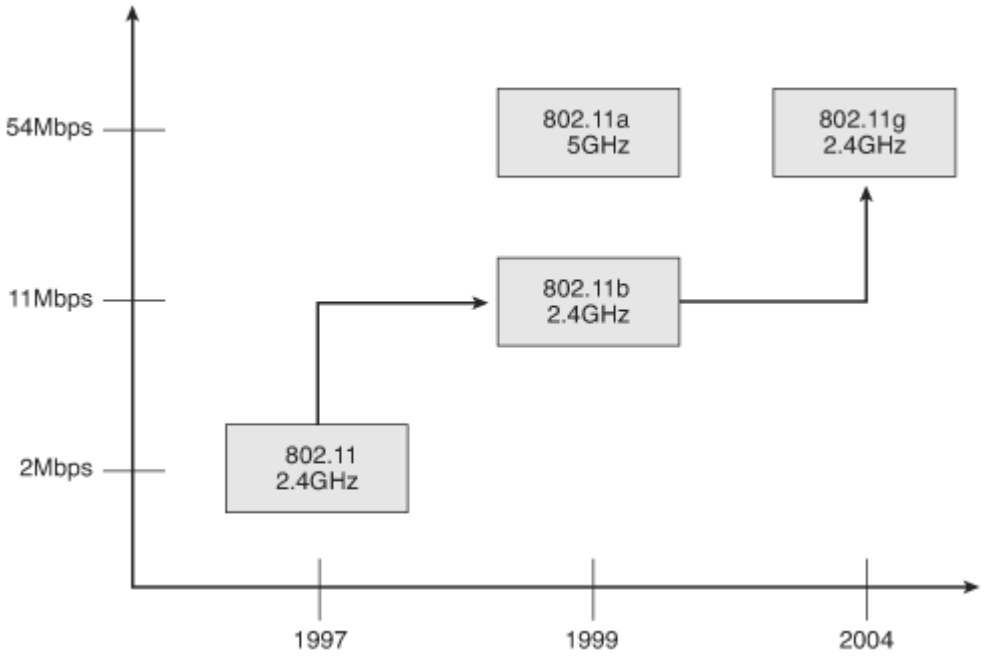

Figura 2-3 – Evolución de las redes 802.11.

2.1.4. Movilidad

Cuando se nombran los aspectos más importantes de una red 802.11, una de los más destacados es la movilidad. Se podría decir que la movilidad es uno de los requisitos más importantes dentro de una red inalámbrica, sea ésta celular o una red 802.11. Una red 802.11 ofrece servicios inalámbricos en una zona determinada, pero se encontrará limitada por el radio de cobertura del punto de acceso. La solución bien podría ser cambiar la antena por una de mayor cobertura, no obstante, esto es impráctico en ambientes interiores por los daños que puede ocasionar el exceso de potencia irradiada por la antena, así como la pérdida de potencia que sufre la señal al encontrar obstáculos.

El estándar 802.11 ofrece una solución mucho más práctica: aumentar el número de puntos de acceso mientras se mantiene la potencia irradiada por las antenas y poner en práctica el roaming. El roaming es un término que difiere según las tecnologías. En el caso de 802.11, aunque no está definido en el estándar oficialmente, es una propiedad de una red 802.11 de dar la libertad a sus clientes de moverse a través de los puntos de acceso manteniendo la conexión. Por supuesto, para ello la red debe contener más de un punto de acceso.

El proceso de handoff se refiere al mecanismo o secuencia de mensajes intercambiados por los puntos de acceso y una estación que da como resultado la transferencia de la conectividad a nivel de la capa física y un estado de la información de un punto de acceso a otro con respecto a la estación en consideración. Así el handoff es una función llevada por al menos tres entidades a nivel de la capa física: la estación, el punto de acceso entrante y el saliente. La información del estado que es transferida típicamente consiste en una credencial del cliente (que le permite el acceso a la red) y otra información. Esta trasferencia puede ser alcanzada por un IAPP, o un Protocolo de Punto de Inter-Acceso, o un protocolo propietario. Para una red IEEE 802.11 que no posee un mecanismo de control de cceso, debe haber una diferencia nominal

entre una asociación completa y un handoff o reasociación. Viéndolo de otra manera, el retardo de un handoff podría ser estrictamente mayor que el retardo de la reasociación debido a que hay una comunicación con un punto de inter-acceso adicional.

La decisión de realizar el roaming se realiza por el cliente. Lo que en realidad hace al cliente realizar un handoff involucra un conjunto de reglas y prioridades determinadas por el fabricante de la tarjeta inalámbrica, usualmente son la potencia de la señal recibida, el nivel de ruido y la BER. Mientras una estación se encuentra conectado a la red, busca continuamente otros puntos de acceso y se autentica con aquellos que se encuentren cerca de su rango. Como se mencionó anteriormente, un cliente puede estar autenticado a varios puntos de acceso pero se encuentra asociado únicamente a uno. Conforme una estación se aleja de un punto de acceso con el que se encuentra asociado y la potencia de la señal decrece, intentarña conectarse a otro punto de acceso y cambiarse de una BSS a otra. Mientras la estación se desplaza, los puntos de acceso por los que pasa se comunican uno con el otro a través del sistema distribuido del medio y ayudan a proveer una transición limpia entre los dos. Muchos fabricantes proveen este tipo de handoff, pero no es oficialmente parte del estándar 802.11, por lo tanto cada fabricante lo hace utilizando su propio método. Dado que cada

proveedor utiliza su propio método de handoff, si una estación se desplaza entre puntos de accesos fabricados por diferentes proveedores, los handoffs suelen provocar retardos de varios segundos.

Todo el proceso del handoff puede ser dividido en dos pasos lógicos diferentes: Descubrimiento y Reautenticación, como se muestra en la Figura 2.3:

Descubrimiento: atribuido a la movilidad, la potencia de la señal y la SNR del punto de acceso al cual se encuentra asociado una estación podría decaer y causar una pérdida de conectividad e iniciar un handoff. En este punto, el cliente podría no estar en la posibilidad de comunicarse con su punto de acceso. De esta forma, el cliente necesita encontrar otros puntos de acceso que se encuentren en rango para asociarse. Esto es posible gracias a una función de la capa MAC: scan o búsqueda. Durante el scan, la tarjeta escucha por mensajes de encuentro beacon (enviados periódicamente por los puntos de acceso cada 10 ms), en los canales asignados. Luego, la estación crea una lista de potenciales puntos de acceso a los cual podría conectarse dependiendo de la potencia de la señal que tengan.

Existen dos métodos de scan definidos en el estándar: activo y pasivo.

Como sus nombres sugieren, en el modo activo, aparte de escuchar por mensajes tipo beacon (método pasivo), la estación envía paquetes adicionales en cada canal y recibe respuestas por parte de los puntos de acceso.

Reautenticación: La estación intenta reatenticarse al punto de acceso de acuerdo a la lista de prioridad. El proceso de reautenticación involucra típicamente una autenticación y una reasociación al punto de acceso posterior. La fase de reautenticación involucra la transferencia de credenciales y otra informació nde estado desde el punto de acceso saliente. Como se mencionó anteriormente, esto se logra gracias a un protocolo como el IAPP.

Reasociación: Finalmente, la estación cambia de punto de acceso con un pedido de reasociación. La conectividad es redirigida al punto de acceso nuevo y perdida desde el inicio del proceso con el punto de acceso saliente.

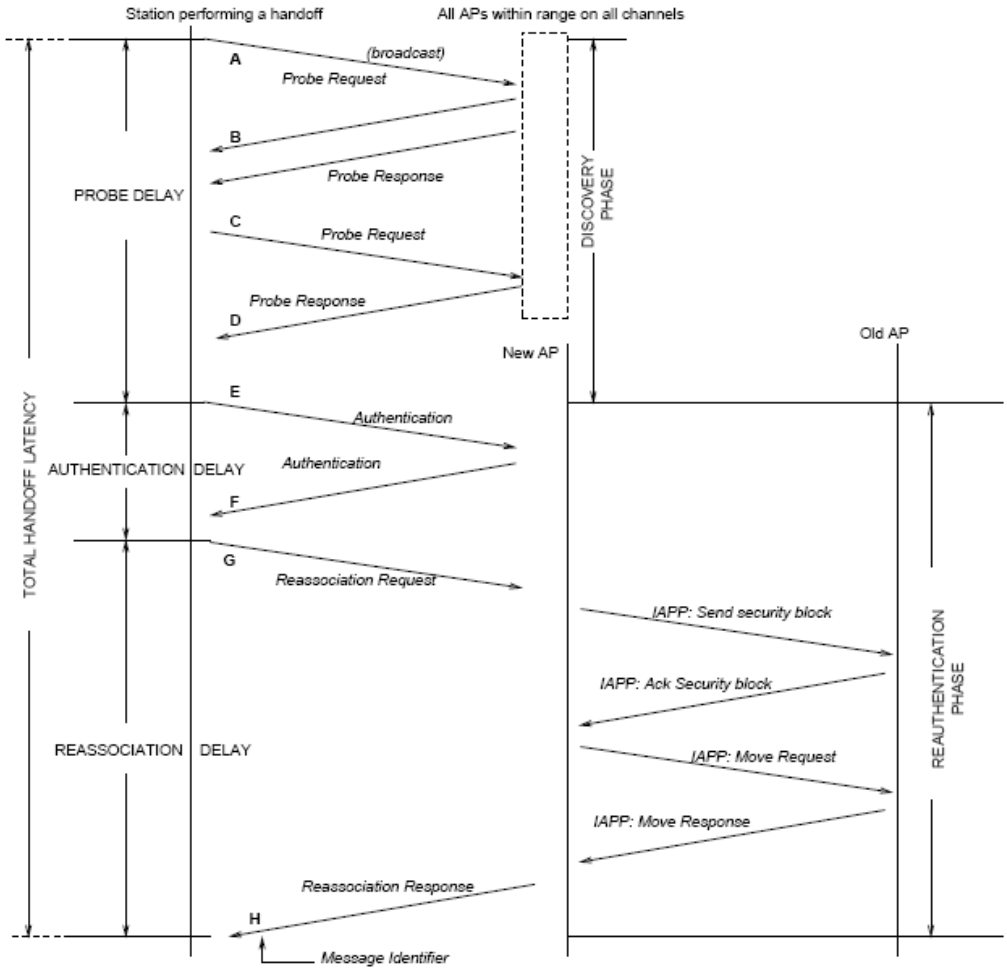

Figura 2-4 - Procedimiento de handoff en una red 802.11 tradicional.

Retardo de mensaje de prueba: Los mensajes desde A hasta E son mensajes de prueba en un scan activo. Consecuentemente, se llama al retardo que existe para este proceso como retardo del mensaje de prueba. El número de mensajes pueden variar de 3 a 11.

Retardo de Autenticación: Este retardo se produce durante el

intercambio de los frames de Autenticación (mensajes E y F). La Autenticación consiste en dos o cuatro frames consecutivos dependiendo del método de autenticación utilizado por el punto de acceso. Algunas tarjetas inalámbricas intenta iniciar la reasociación antes de la autenticación, lo cual introduce un retardo adicional al proceso de handoff y además resulta ser una violación al estado IEEE 802.11 de la máquina.

Retardo de Reasociación: Este retardo se produce durante el intercambio de los frames de reasociación (mensajes G y H). Luego de una autenticación exitosa, la estación envía una petición de reasociación y completa el handoff.

2.2. Las Redes Wireless Mesh

2.2.1. Definición y Arquitectura

Una red Wireless Mesh (WMN) es una red 802.11 formada por puntos de acceso cuya topología de red es la unión de una topología amallada (Mesh) con una topología infraestructura. En una WMN, la mayoría de puntos de acceso se comunican entre sí mediante un enlace inalámbrico, mientras que una porción minoritaria actúan de backhaul a la red cableada, de existir. El área de cobertura de los nodos trabajando

como una red es usualmente llamada "nube mesh". El acceso a esta nube mesh es dependiente de la armonía de los nodos trabajando en conjunto para crear la red. Una de las características más importantes es su capacidad de auto curarse: en caso de que uno o más enlaces se vean afectados, los routers vecinos reconfiguran el esquema de la red de tal modo que ningún nodo pierda conectividad.

Su arquitectura puede variar dependiendo de la aplicación, no obstante, se identifican tres elementos comunes en la red:

Punto de Acceso Mesh: Es un nodo que se encarga del enrutamiento, así como de ofrecer los servicios inalámbricos a las estaciones. Mantiene constante comunicación con otros puntos de acceso mesh de la red. Todo Router Mesh es un punto de acceso mesh.

Punto Mesh: Es un nodo que repite los paquetes para redirigirlos a los puntos de acceso Mesh y participan sólo en comunicaciones de un salto. Para ello establece enlaces punto a punto con Puntos Mesh vecinos o Puntos de Acceso Mesh.

Puerta de Enlace Mesh: Conecta a la red inalámbrica mesh con una red LAN. Son prescindibles en tanto no sea necesario conectarse con una

red externa a la red Mesh. No obstante, son bastante utilizados en la práctica.

Cliente Mesh: Es la estación definida en 802.11.

2.2.2. Movilidad

Una de las características principales de una WMN es que contienen pocas puertas de enlace conectadas a una LAN mientras que los routers inalámbricos proveen acceso a los clientes mesh. Dentro del rango de un router mesh, el cliente puede desplazarse libremente, no obstante, conforme se aleja de él y se acerca a otro router mesh, debe realizar un handoff para conservar la conectividad.

Las redes mesh inalámbricas mantienen el mismo concepto de Descubrimiento y Reautenticación como las redes 802.11 tradicionales, no obstante, la movilidad se encuentra ciertamente limitada, en un sentido amplio, por los overheads o la sobrecarga de paquetes transmitidos en la red, pero que resultan ser vitales para la supervivencia de la red mesh, y que son enviados por los protocolos de enrutamiento para el monitoreo del estado de la red. Por ello se puede decir que la implementación de una red mesh puede tener una

desventaja sobre una red WLAN 802.11 común basados en la movilidad. No obstante, este punto puede revertirse al momento de analizar la mejor ruta, considerando que una red 802.11 debe enrutar los paquetes a través de la red de área local a la cual se encuentra conectado cada uno de los puntos de acceso, por lo que el tráfico de la LAN suele ser un punto desfavorable en el througput esperimentado por una externalidad a la red inalámbrica.

Básicamente funciona bajo el estándar 802.11, y por lo tanto el proceso se lleva a cabo en tres etapas: Descubrimiento, Reautenticación y Reasociación. Basado en la naturaleza de los pasos, se puede resumir en dos fases: la fase de escaneo y la fase de ejecución.

La Figura 2.4 resume el proceso de Handoff en una red Mesh.

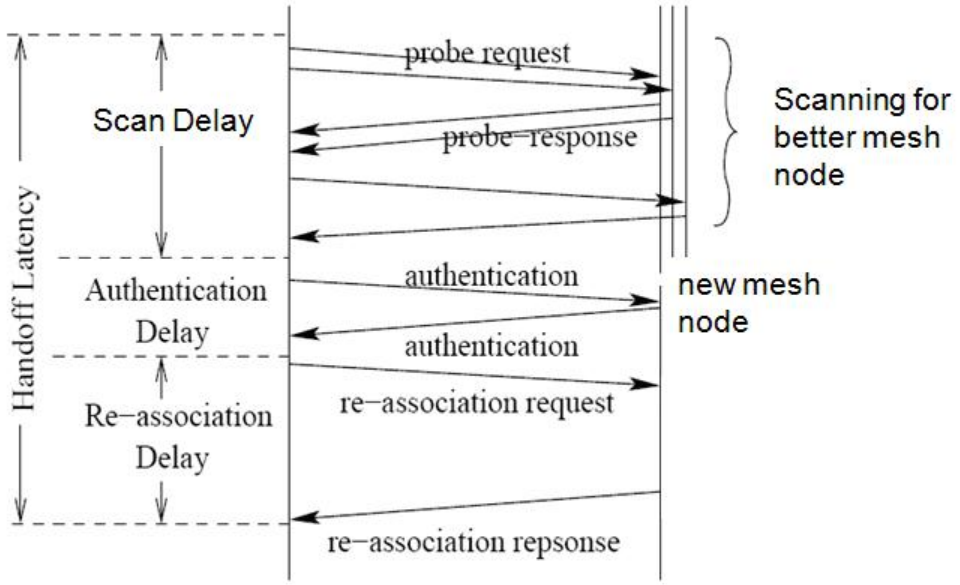

Figura 2-5 - Proceso de Handoff en una red mesh inalámbrica.

Fase de escaneo:

Scan Pasivo: Requiere al menos de 100 ms para cada canal, lo cual bien podría requerir de 1.3 segundos en escanear todos los canales disponibles en Europa.

Scan Activo: El tiempo esperado por canal es minimizado.

$$TiempoCanalMinimo = DIFS + (aCW\ \min * tiempoSlot)$$

tiempoSlot definido en el estándar a 20us en 802.11b/g y 9us en 802.11a. TiempoCanalMaximo es el tiempo máximo que debe esperar

por una respuesta a un paquete de prueba cuando un canal está siendo utilizado

Fase de ejecución: El retardo en esta fase es la suma de los retardos de Autenticación y Reasociación. 802.11r tiene la tarea de minimizar el retardo en esta fase para satisfacer los requerimientos de aplicaciones en tiempo real.

2.2.3. Protocolos de Enrutamiento

El enrutamiento en WMN y en Redes Ad-Hoc utilizan el mismo concepto clave: comunicación entre nodos a través de múltiples saltos. Las redes Ad-Hoc Móviles (MANETs en inglés) tienen un fin académico y enfoque sobre los dispositivos usuarios, movilidad y capacidades Ad-Hoc. Las WMNs tienen un contraste comercial y está enfocado en dispositivos estáticos, confiabilidad, capacidad de la red y en la implementación. La funcionalidad principal de una red WMN es la capacidad de enrutamiento. Los protocolos de enrutamiento proveen los caminos necesarios a través de una Red Mesh Inalámbrica, de tal modo que los nodos puedan comunicarse a través de los mejores caminos en múltiples saltos. Los protoclos de enrutamiento deben tener en cuenta la

dificultad en los constantes cambios en el ambiente y deberían brindar una comunicación confiable y eficiente para la red mesh.

Debido a que las Redes Mesh Inalámbricas comparten características con las Redes Ad-Hoc Inalámbricas, los protocolos de enrutamiento para las MANETs pueden ser aplicados a las WMNs. Con cierta frecuencia, los conceptos principales de los protocolos de enrutamiento existentes son extendidos hasta satisfacer los requerimientos especiales de las Redes Mesh Inalámbricas, como en el caso de las métricas de radio en 802.11s.

A pesar de la disponibilidad de una cantidad considerable de protocolos de enrutamiento para Redes Ad-Hoc, el diseño de protocolos de enrutamiento para WMNs se encuentra constantemente bajo investigación por diferentes motivos:

En la mayoría de WMNs, muchos de los nodos son o bien estacionarios, o tienen una movilidad mínima y no dependen de una batería. De este modo, el enfoque de los algoritmos de enrutamiento se dirige a mejorar el desempeño de la Red, en lugar de minimizar el uso de energía.

La distancia entre los nodos es normalmente menor, lo cual incrementa la calidad del enlace y la tasa de transmisión. Sin embargo, distancias cortas también incrementan la interferencia entre saltos, lo cual además baja el ancho de banda por enlace. Por lo tanto, es necesario descubrir nuevas métricas que mejoren el desempeño de los protocolos de enrutamiento en WMN multiradio.

En una WMN multiradio, el protocolo de enrutamiento no solamente necesita seleccionar un camino entre diferentes nodos, sino que necesita también seleccionar el canal más apropiado por nodo mesh. Por consecuencia, las métricas de enrutamiento tienen que ser descubiertas y utilizadas para tomar ventaja de múltiples radios en una WMN.

Basados en el deseméño de un protocolo de enrutamiento existentes para Redes Ad-Hoc inalámbricas y los requerimientos mínimos de las WMNs, un protocolo de enrutamiento óptimo debe tener en consideración lo siguiente:

- **Tolerancia a fallas:** Una de las características más importantes de una Red Mesh Inalámbrica es su capacidad de funcionar incluso en condiciones desfavorables provocadas por fallas en

los enlaces entre nodos. El protocolo debe asegurar robustez frente a fallos presentados en la red, lo cual se traduce en el replanteamiento de rutas alternativas en caso de que uno o más enlaces fallen.

- **Balance de Carga:** Los Routers Mesh inalámbricos son excelentes en balancear la carga, al tener la libertad de elegir el camino más eficiente para enrutar los paquetes.
- **Reducción de Overhead:** La conservación de ancho de banda es imperativa para el éxito de cualquier red mesh inalámbrica. Es importante reducir el overhead en el enrutamiento, especialmente el causado por los broadcasts.
- **Escalabilidad:** Una red mesh es escalable y puede manejar cientos o miles de nodos. Debido a la operación de la red, no depende de un punto central de control, añadiendo muchos puntos de recolección de datos, o puertas de enlace es muy conveniente.
- **Soporte QoS:** Debido a las capacidades limitadas de canal, la influencia de la interferencia, el gran número de usuarios y la cada vez mayor cantidad de aplicaciones multimedia, soportar calidad de servicio se ha convertido en un requerimiento crítico en una red WMN.

Ad hoc On-demand Distance Vector Routing

AODV es un protocolo de enrutamiento muy popular en las MANETs. Los routers se configuran en "demanda", y sólo se mantienen routers activos. Esto reduce el overhead de enrutamiento, pero introduce cierto retardo inicial debido a la configuración basada en demanda. Existen varias implementaciones disponibles, por ejemplo, AODV-UU de la Universidad de Uppsala. Recientemente, una adaptación de AODV ha sido propuesta para redes mesh inalámbricas.

AODV utiliza un mecanismo simple de requerimiento-respuesta para el descubrimiento de las rutas. Puede utilizar mensajes hello para mantener a los nodos informados sobre la conectividad con sus vecinos o fallas en los enlaces. Cada información de enrutamiento tiene un tiempo de vencimiento asociado así como un número de secuencia. El uso de números de secuencia permite detectar datos desactualizados o anteriores, de modo que se utilizan los datos más actuales y disponibles. Esto evita problemas comunes en otros protocolos basados en distancia en los que se encuentran en lazos infinitos de conteo.

2.2.4. Ventajas y desventejas sobre WLANs tradicionales

Desde sus inicios, las Redes Wireless LAN fueron diseñadas con la finalidad de extender una red LAN utilizando el medio inalámbrico. No obstante, han evolucionado al punto de desarrollar cierta independencia de una red cableada, aunque este no sea, incluso actualmente, el pico de su utilidad. Las Redes Wireless Mesh son un claro ejemplo de dicha evolución: representan el máximo exponente de la independencia de una red LAN al no ser una añadidura de una Red LAN.

En términos de topología e implementación, las redes mesh inalámbricas presentan una notable ventaja al no precisar de una infraestructura cableada a lo largo de toda la red para funcionar. En su lugar, la conectividad se lleva a cabo por el medio inalámbrico. Esto representa un ahorro en costos de implementación, tiempo de instalación aunque se sacrifique cobertura.

2.2.5. Uso y Aplicación de las redes Wireless Mesh

Las redes mesh inalámbricas son utilizadas ampliamente por los municipios de varias ciudades del mundo con diversos fines. Uno de los princiaples objetivos es crear redes de vigilancia conectando cámaras se seguridad en postes. Como es de imaginarse, resulta mucho más

oportuno implementar una red mesh inalámbrica dado que implementar una red 802.11 supone el uso de una LAN adicional.

Las redes mesh también son utilizadas para extender la conectividad a Internet en ciudadelas o entornos metropolitanos. En España, sólo en Avilés, 2007 y Zaragoza, en 2008 se han desarrollado grandes redes mesh metropolitanas con soporte para VoIP y movilidad gracias al impulso de los municipios.

Las aplicaciones de video vigilancia con Wireless Mesh Networks se ha popilarizado en áreas metropolitanas en algunas ciudades de Estados Unidos. Empresas como Firetide o Aruba Networks trabajan no sólamente en el diseño e implementación, sino también en la fabricación de equipos de Wireless Mesh Network Surveillance (Sistemas de Vigilancia con Wireless Mesh Networks).

2.3. La Voz sobre WLAN

Dentro del abanico de soluciones que se pueden integrar a una red WLAN, se encuentra la transmisión de voz. Como se mencionó anteriormente, el envío de voz por el medio inalámbrico conlleva a un conjunto de problemas relacionados a Calidad de Servicio, no obstante,

conforme se establecen nuevos mecanismos de conexión, así como nuevas soluciones a handoffs, es posible mejorar la Calidad de Servicio en la Voz sobre WLAN.

Los sistemas VoWLAN son una extensión a los sistemas de Voz sobre IP y una alternativa a las comunicaciones de Voz digital y analógica. La VoWLAN ofrece beneficios significantes de proveer movilidad y convergencia de voz y datos. Con las redes VoWLAN, los hospitales, empresas, universidades, tiendas grandes, almacenes, entre otras posibles soluciones.

2.3.1. Características

Arquitectura

Los elementos que participan dentro de un sistema de VoWLAN son una combinación efectiva de los elementos de tanto las redes VoIP como de las redes WLAN. La figura 2.5 muestra los elementos de una WLAN. Gracias a que ambos sistemas trabajan en diferentes capas y servicios, son perfectamente compatibles. Sus principales son:

- **Wireless IP Phone:** Muy similar a un teléfono celular, no obstante incluye un adaptador de redes inalámbricas 802.11 para conectarse a una red WLAN. De igual forma como un teléfono IP convencional (Ethernet), es capaz de registrarse en una red VoIP y realizar/recibir llamadas de la red en cuestión, así como a la red PSTN externa. Un número considerable de teléfonos celulares incluyen una tarjeta de red 802.11 en la actualidad. Con ello pueden conectarse a una red WLAN y por consiguiente a una red VoWLAN mediante una aplicación móvil.
- **Call Manager:** Toma el lugar de una PBX para procesar las llamadas dentro de la red, así como la tarea de registrar extensiones, administrar correo de voz, entre otras funciones más complejas. Constituye el corazón del sistema y el controlador del tráfico y direccionamiento de las llamadas.
- **Voice Gateway:** Se encarga de servir como interfaz al protocolo de Internet frente a otros sistemas y redes. Sirve de traductor de mensajes y protocolos entre redes VoIP y PSTN. Hoy en día los Gateways de Voz se encuentran integrados en los Call Managers.
- **Infraestructura WLAN:** El medio por el cual se transmiten las llamadas de la red. Salvo a excepciones, debido a que el la infraestructura VoIP se encuentra en la red LAN, es indispensable que al menos un nodo de la red WLAN se encuentre conectado a la red LAN a la cual se encuentra conectado el Call Manager.

El adaptador de red en el teléfono IP del usuario debe conectarse a un punto de acceso en la red antes que el usuario pueda realizar llamadas. Luego de ello, el cliente se registra en la PBX. Para ello, el cliente debe enviar ciertos parámetros básicos que deben ser conocidos por ambas partes, tales como el número de extensión y la clave secreta para registrarse. Una vez finalizado el registro, la PBX tiene el conocimiento de la dirección de red donde puede contactar al cliente en caso de una llamada entrante, así como redireccionar las llamadas.

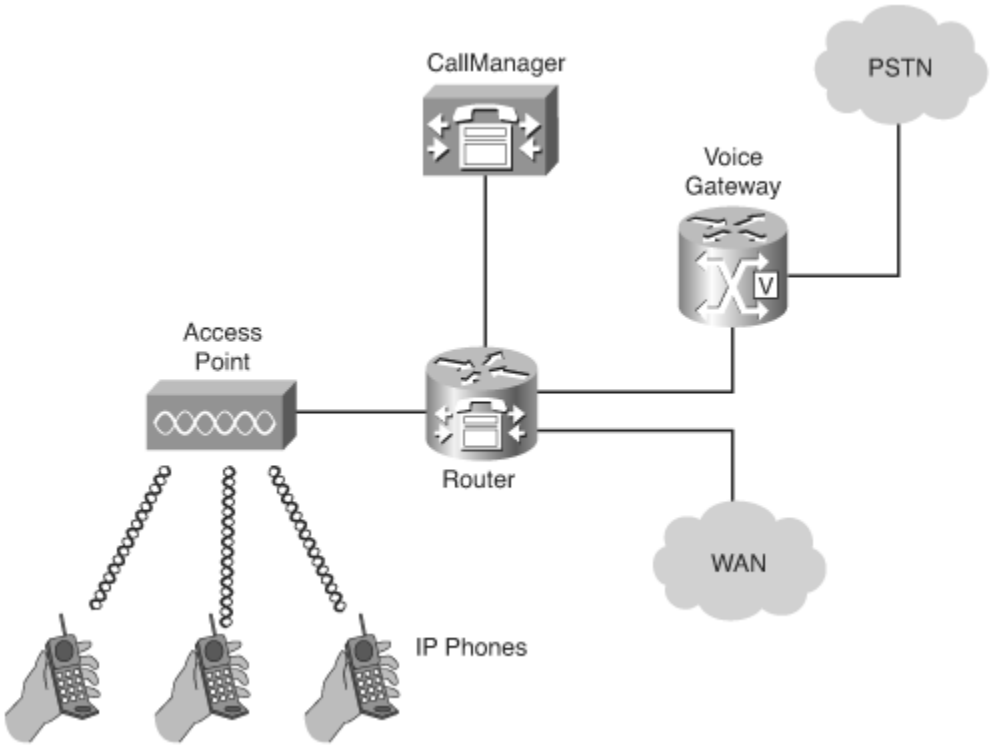

Figura 2-6– Arquitectura de una red VoWLAN.

2.3.2. Movilidad

Si bien es cierto, anteriormente en el presente trabajo se ha tocado el tema de la movilidad y se ha determinado que es una característica intrínseca de las redes WLAN, que son quienes manejan la conectividad. No obstante, la movilidad se encuentra limitada por la Calidad de Servicio.

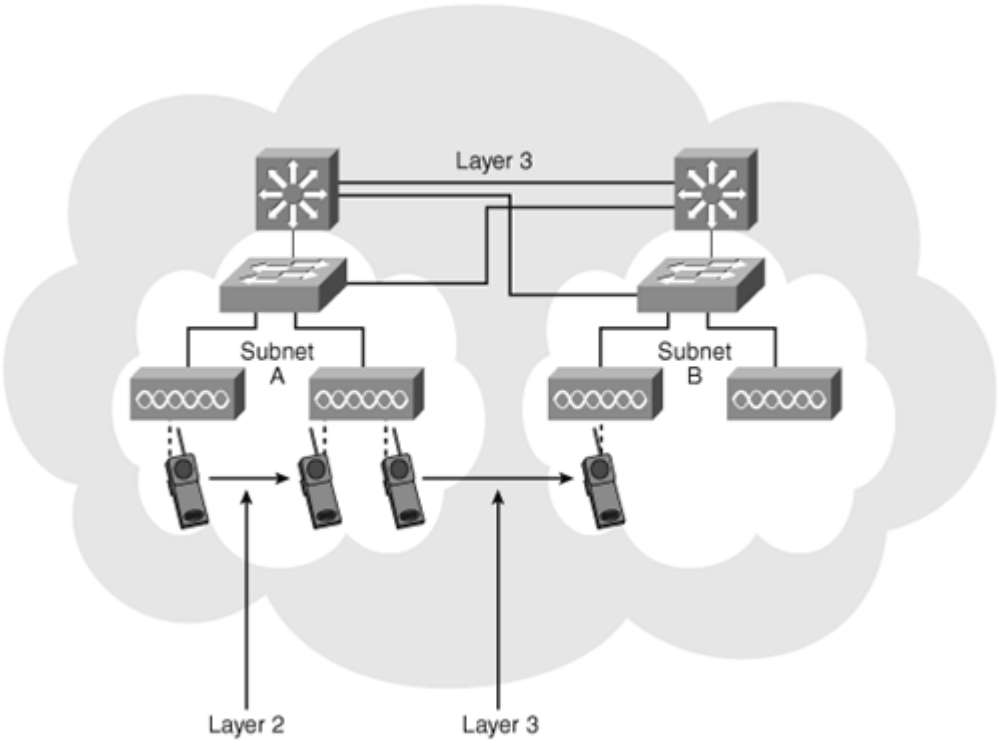

Figura 2-7– Movilidad de un cliente a través de una red VoWLAN.

La movilidad durante una llamada es también conocida como "mid-call roaming". Para evitar que una llamda se pierda por la latencia experimentada durante el desplazamiento entre nodos, es necesario

que el handoff asociado sea lo más pronto posible. Por ello es necesario prestar primordial importancia al diseño de la infraestructura de la Red.
En implementaciones de VoWLAN es muy común encontrar un gran número de soluciones dependiendo del espacio físico en el que se implementa una red VoWLAN. En primera instancia, es posible seccionar la nube completa de VoWLAN en Subredes o VLANs diferentes por área, dependiendo de los requerimientos.

Por otro lado, es posible considerar la movilidad como una propiedad de la VoWLAN y que se encuentra determinada por la misma capacidad de la red de permitir handoffs efectivos y sin mayores complicaciones, tales como retardos excesivos o incapacidad del sistema por reasociar un cliente a un nuevo punto de acceso. Ahora bien, la medida relacional de la movilidad en una red VoWLAN se encuentra en el número de llamadas perdidas. En cuanto una llamda se encuentre en curso, la movilidad (que hasta cierto punto puede considerarse como calidad) está determinada por: de calidad de comunicación, ya que en movimiento las condiciones de conectividad cambian y que está mucho más relacionado a la naturaleza del medio y de la red; y la cantidad de llamadas perdidas, que se trata de el número de clientes que puede soportar la red a la vez, sin desmejorar la calidad de comunicación por individuo.

De esta forma, la capacidad que tiene un cliente para trasladarse a través de una red VoWLAN se encuentra fuertemente relacionada con las características del medio y de la red.

2.3.3. Ventajas y Desventajas sobre la Voz sobre IP tradicional.

Ambas redes son complementarias en cuanto una brinda características que la otra no posee o que no es intrínseca en su naturaleza. En primera instancia, instalar una red VoWLAN implica necesariamente conectarse a una LAN, que cuente con una red VoIP funcional (lo cual sucede en la mayoría de los casos), funcionando de esta manera como una extensión a una red cableada. Salvo algunas excepciones en las que es posible instalar una PBX open source en un nodo de la red, para poder contar con una red VoWLAn es estrictamente necesario contar con una red LAN en donde funcione la PBX que administre el tráfico VoIP en la red. Es decir, una red VoWLAN carece de autonomía absoluta, al depender de una red VoIP cableada tradicional.

Por otro lado, la Calidad de Servicio se ve afectada de diferentes formas en ambos casos: el medio de transmisión en una red VoIP cableada tradicional es el cableado Ethernet (o el disponible). No así, en una red

VoWLAN a esto se suma el medio inalámbrico. Esto implica retardos adicionales que complican la Calidad de Servicio verificada en las llamadas.

No obstante, uno de las motivaciones más poderosas para utilizar la VoWLAN se encuentra en su característica más importante: la movilidad.

Otra de las grandes ventajas de la VoWLAN es la capacidad de muchos teléfonos celulares de contar con tarjetas de red inalámbricas y software que les permiten registrarse en una red VoIP, y consecuentemente recibir llamdas. Con ello, se diversifica el uso de dichos dispositivos, al punto que sea posible prescindir de teléfonos WiFi. De este modo, es posible mantenerse conectado a ambas redes (celular y VoWLAN) con un mismo dispositivo. El uso alternativo de un dispositivo tecnológico es una clara ventaja para la VoWLAN.

2.3.4. Consideraciones especiales de diseño e implementación.

Esta sección trata de los elementos técnicos que necesitan ser tomados en cuenta al diseñar una red VoWLAN.

El proceso de diseño de cualquier sistema descubre elementos técnicos que juntos explican cómo el sistema satisfacerá los requerimientos. Los pasos necesarios para diseñar una red VoWLAN son:

Paso 1: Especificar la arquitectura completa del sistema. Este paso involucra la selección de un modelo previamente probado que indique cómo interactuan los componentes necesarios, especificando cómo funcionarán los handoffs, determinando la seguridad y los elementos de Calidad de Servicio (QoS) y definiendo la infraestructura de la red.

Paso 2: Identificar las localizaciones de instalación de los puntos de acceso. Este paso involucra realizar pruebas dentro del lugar de implementación a fin de identificar los lugares óptimos de instalación para cada punto de acceso.

Paso 3: Documentar el diseño. Este paso es muy importante, por cuanto es una referencia al instalarlo y al darle soporte.

Site Survey

Se denomina Site Survey al proceso de diseño y planificación de una red inalámbrica con el objetivo de proveer una solución inalámbrica con

parámetros adecuados de cobertura, tasas de tansmisión, capacidad de la red, movilidad y QoS. Los sites surveys suelen involucrar una visita al lugar para realizar pruebas que indiquen las posibles fuentes de interferencia y canales disponibles.

En sistemas inalámbricos, predecir la propagación de ondas de radio y detectar la presencia de señales de interferencia sin el uso de equipo para realizar pruebas es difícil. Incluso si se utiliza antenas omnidireccionales, las ondas electromagnéticas no recorren las mismas distancias en todas las direcciones. En su lugar, obstáculos como puertas, paredes, personas, elevadores, entre otros, ofrecen diferentes grados de atenuación, lo cual cambia los patrones de radiación RF a un punto de considerarse irregulares e impredecibles. Como resultado, realizar un site survey es en muchos casos necesario para comprender completamente el comportamiento de las ondas de radio dentro de un establecimiento antes de efectuar la instalación de los puntos de acceso.

El objetivo definitivo de un site survey es brindar la información necesaria para determinar el número y ubicación de puntos de acceso que provean una cobertura adecuada a través del lugar en cuestión. Un site survey también detecta la presencia de interferencia proveniente de

otras fuentes que pueden degradar el desempeño de una red inalámbrica.

La necesidad y complejidad de un site survey varía dependiendo del lugar. Por ejemplo, una oficina pequeña de tres cuartos quizás no requiere de un site survey. Este escenario podría solucionarse con un solo punto de acceso (o más, dependiendo de el número de usuarios). Un lugar mucho más amplio como una universidad, un edificio, hospital, etc. generalmente requieren un site survey. Sin un site survey, los usuarios pueden experimentar falencias como falta de cobertura y tasas de transmisión adecuadas.

Cuando se conduce un site survey, es necesario seguir las siguientes tareas:

- Obtener un diagrama del lugar donde se realizan las pruebas.
- Inspeccionar visualmente el lugar. Con ello es posible identificar posibles barreras que afecten la propagación de señales RF. Por ejemplo, una inspección visual puede descubrir obstáculos como metales, microondas o lugares que brinden una atenuación adicional.

- Identificar áreas de usuarios: en el diagrama, identificar los lugares en los cuales los usuarios harán uso de la red.
- Determinar zonas preliminares donde pueden ser ubicados puntos de acceso. Esto luego de considerar el punto anterior, donde se ubican las zones de mayor tráfico y donde los usuarios harán uso de la red.
- Reunir las herramientas necesarias: se necesita al menos un punto de acceso para servirse de pruebas. Se recomienda configurar el punto de acceso con las mismas configuraciones de la red en general. Utilizar las herramientas de pruebas para identificar la cobertura del punto de acceso, así como la intensidad de señal detectada proveniente de otros puntos de acceso

En el presente trabajo se considera un TestBed para realizar pruebas. Es necesario, por consiguiente, realizar un site survey es de vital importancia para conocer las condiciones del medio y, por consiguiente, considerar posicionamiento de puntos de acceso, canales a utilizar y tomar en cuenta los posibles niveles de interferencia para inferir luego de los resultados.

2.4. Calidad de Servicio

La Calidad de Servicio es un concepto aplicado a todas aquellas tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado. En escenarios inalámbricos es escencialmente importante realizar un estudio de QoS, no obstante, muy hostil para realizar medidas debido a su variabilidad en el tiempo. Esto implica que satisfacer la QoS resulta imposible en el 100% de los casos. Los sistemas de comunicaciones estandarizados pueden sólo garantizar los requerimientos para un determinado porcentaje (diferente de 100%).

2.4.1. Importancia

El uso de técnicas para medir QoS asegura una comunicación fiable y nítida para la mayoría de los casos. Los parámetros que se miden en las pruebas de QoS describen objetivamente el estado de la red gracias a que brindan cifras que permiten tomar decisiones para mejorar o realizar optimización.

En las redes de telefonía celular, asegurar una QoS adecuada a la Red es de vital importancia. La experiencia del usuario al utilizar la red, ya sea para llamar o enviar datos, es la prueba definitiva del funcionamiento de la red. De la misma forma, en la instalación de una

Red VoIP convencional, el estudio de QoS asegura que todos los clientes tengan una experiencia de uso de la red positiva.

En el caso de la VoIP sobre WLANs es aún más crítico el estudio de la QoS. Si bien es cierto, la experiencia del usuario al realizar llamadas de VoIP tradicionales debe ser positiva, en el caso de el medio inalámbrico, la utilidad de las pruebas de QoS permiten, de igual forma, comprender la naturaleza de la red y realizar cambios si es necesario.

Por otro lado, y con respecto a la presente tesis, el estudio de la Calidad de Servicio permite seleccionar la solución cuyo comportamiento sea el más adecuado para un entorno establecido.

2.4.2. Tipos de Mediciones

Existen básicamente 2 tipos de mediciones: subjetivas y objetivas. Ambas necesitan seguir procedimientos específicos en pro de reunir los datos suficientes para llegar a conclusiones definitivas sobre el comportamiento de la implementación de una red.

2.4.2.1. Subjetivas

Las mediciones subjetivas son aquellas que se efectúan desde el punto del usuario, el cual califica la experiencia que ha tenido al utilizar la red para realizar llamadas, en este caso, de VoIP sobre WLAN. Es importante resaltar que el usuario no sigue soluciones técnicas que puedan tener un impacto directo en las mediciones y, por tanto, se basa únicamente en la apreciación (subjetiva) durante las pruebas.

2.4.2.2. Objetivas

Las mediciones objetivas son aquellas cuyos datos pueden cuantificarse directamente desde la tarjeta de red. Aunque no están directamente relacionados con el usuario, es posible establecer un margen de fiabilidad fijando parámetros límites aceptables y, por tanto, establecer objetivamente si la red es efectivamente fiable para la comunicación.

2.4.3. Métricas

Las métricas constituyen los tipos de datos que se recopilan durante las pruebas. Existen una variedad considerable de métricas disponibles, no obstante, son básicamente cuatro las más importantes: jitter, delay, packet loss y bandwidth explicados a continuación.

2.4.3.1. Jitter

Jitter es la variación de señal periódica en el tiempo. Medir Jitter en redes de VoIP es útil para conocer la variabilidad de la latencia (Delay) de los paquetes a través de la red. El jitter de paquetes es expresado como la media de la variación de la latencia promedio de la Red. El jitter es un parámetro cuya utilidad radica en conocer qué tan variable es la red en estudio: a mayor Jitter, la variación de la latencia en la red es mayor.

2.4.3.2. Delay

La latencia (Delay) de un paquete es el tiempo que se demora dicho paquete en llegar a su destino. Es uno de los parámetros más importantes (si no es el de mayor importancia). Un delay muy alto implica escuchar una versión atrasada del audio proveniente del emisor, lo cual complica la comunicación al punto que es imposible llevar una conversación fluida. Por ello, es de vital importancia tomar muy en cuenta la cantidad de delay en el transcurso del diseño e implementación de una red.

2.4.3.3. Packet Loss

Packet Loss se refiere a la pérdida de paquetes en la red. Los paquetes normalmente pasan por uno o varios routersy, en casos no comunes, dichos routers pueden cometer errores de enrutamiento o sufrir de saturamientos momentáneos. Además, el medio inalámbrico, al ser inestable, puede contribuir a la pérdida de paquetes debido a interferencias o puntos ciegos, impidiendo así la correcta entrega de información.

2.4.3.4. Bandwidth

Diferente a los casos anteriores, es de esperarse que la cantidad de ancho de banda sea alta y constante para llamadas de VoIP. Es deseable asimismo que la cantidad de ancho de banda utilizado por la red sea suficiente para asegurar un número específico de llamadas antes de que ya sea la PBX o la red se congestionen.

2.4.4. Parámetros Ideales

Así como es importante conocer los parámetros útiles para medir el desempeño y abrir las puertas a mejorar una red determinada, es también importante conocer los parámetros recomendados por la ITU

para asegurar una comunicación fluida y una buena experiencia de usuario. Es importante recalcar que para el caso del delay, packet loss y jitter es necesario que sean lo más bajos posible. No así, el ancho de banda (bandwidth) debe mantenerse en un nivel constante. Los valores correspondientes a los recomendados por la ITU están descritos en la tabla I.

Parámetro	Valor
Delay	No mayor a 150 ms
Jitter	100 ms, rec: 30 ms
Ancho de Banda (G711)	80 kbps
Packet Loss	1.00%
Call Drop	10.00%

Tabla I - Parámetros y Requerimientos en VoIP

CAPÍTULO 3

3. IMPLEMENTACION DE UN TESTBED QUE PERMITA REALIZAR UN ANALISIS COMPARATIVO DE LA IMPLEMENTACION DE LA VOZ SOBRE UNA RED WIRELESS MESH CON SOLUCIONES COMUNES VERSUS EL USO DE SMESH.

Para probar la efectividad de las redes de acuerdo a lo establecido en la hipótesis, es necesario llevar a cabo una serie de experimentos con cada solución disponible. Para ello es fundamental primero implementar redes de prueba, o un Testbed. El presente capítulo detalla las características de dicho Testbed, así como la manera en la cual las redes son implementadas, el hardware y el sofware utilizado y la secuencia de experimentos a desarrollarse.

3.1. Consideraciones técnicas

Para realizar efectivamente pruebas de Calidad de Servicio en VoWLAN, es necesario tomar en consideración los elementos que participan en la implementación de una Red WLAN, atendiendo los parámetros necesarios para crear un entorno ideal para la transmisión de datos, calidad de señal entre nodos, niveles de interferencia, entre otros elementos clave.

No obstante, es necesario tomar en cuenta que existen diferencias entre la implementación de un TestBed y una solución comercial específica. Un TestBed es una plataforma de expermientación que sirve para realizar pruebas sobre un tema en específico, basado en un marco teórico y que, por tanto, sirva de medio para refutar o comprobar una teoría. Para la implementación del TestBed es fundamental orientar las predicciones teóricas de acuerdo al medio en el que se llevan a cabo las pruebas. Por otra parte, la implementación de una red WLAN funcional supone el esfuerzo por optimizar las condiciones en las que se lleva la comunicación (para este caso específico) en el supuesto que se ha previamente demostrado que una solución determinada satisface las demandas de ciertos requerimientos previamente especificados.

En el presente trabajo, se utiliza un TestBed que tiene como finalidad comprobar o refutar la Hipótesis previamente planteada: "La Calidad de

Servicio en Voz sobre Redes Inalámbricas se ve mejorada con el uso de SMesh en comparación con el uso de otras redes tradicionales Wireless Mesh y Wireless LAN tradicionales dentro de instalaciones de la FIEC".

Para la implementación del TestBed aplicado a la hipótesis planteada, se ha tomado en consideración lo siguiente:

3.1.1. Elementos que participan.

El universo de elementos que participan en el TestBed puede dividirse en 3 partes importantes: el medio en el que se realizan las pruebas, el hardware y el software utilizado.

3.1.2. Medio en el que se realizan las pruebas.

Comprende el espacio físico en el cual se relizarán las pruebas, así como los detalles específicos del mismo. En el caso del Testbed presentado, el lugar escogido es un recorrido que parte desde el antiguo laboratorio de telecomunicaciones (alado del laboratorio de electrónica) hasta el antiguo edificio del decanato y secretaría de la FIEC.

El recorrido escogido se debe principalmente a la cercanía con el antiguo laboratorio de telecomunicaciones, lugar donde funcionaba el programa VLIR que auspicia el proyecto relacionado a la presente tesis:

"STUDY AND DESIGN OF A SOLUTION TO HANDOFF ISSUES EXPERIMENTED IN VOICE OVER WIFI COMMUNICATION OPTIMIZING QUALITY OF SERVICE PRIOR TO THE IEEE 802.11R STANDARDIZATION".

Para ello es necesario realizar un site survey con el objetivo de identificar la naturaleza del medio en el que se realizarán las pruebas mientras se reune la información necesaria para darle forma al Testbed. Conocer la posición de los nodos que sirven las redes presentes en el momento del Site Survey es también importante. Aunque ambas medidas no son concluyentes matemáticamente hablando, dan una pista del lugar donde se pueden situar los puntos de acceso para las pruebas respectivas.

Hardware utilizado.

El Hardware utilizado para las pruebas lo conforman: puntos de acceso, clientes prueba y la centralita (PBX) que administra las llamadas. En el caso de los clientes de prueba y la centralita, son los mismos para todas las pruebas. No así, los puntos de acceso son diferentes de acuerdo a la solución planteada.

La Centralita (PBX)

La Centralita funciona como Call Manager, que es la pieza dentro de la estructura del Testbed encargada de administrar las llamadas entre las extensiones de prueba. La Centralita es importante en las pruebas dado que es un elemento fundamental en cualquier red VoWLAN. Prescindir de una Centralita implicaría restar latencias que alejarían las soluciones de casos reales. Para las pruebas, la centralita escogida es Asterisk, una solución open source que implementa las funcionalidades de una central telefónica PBX en un computador. En la Tabla II se puede apreciar las características de la PC donde se instaló Asterisk.

Característica	Valor
CPU	GenuineIntel Intel(R) Celeron(R) CPU 2.00GHz
Disco Duro	80 GB
Memoria RAM	512
Utilización promedio CPU	7.63%
Sistema Operativo	CentOS 5

Tabla II - Especificaciones del Servidor

Se registran 3 extensiones en Asterisk que serán utilizadas por los clientes móviles. La PC tiene dos interfaces de red: una con una dirección pública y otra con una dirección privada. La dirección privada es utilizada para realizar las pruebas, mientras que la dirección pública

permite acceder desde un punto remoto a la interfaz Web de configuración. Los detalles de las direccioens de red utilizadas en las pruebas están detalladas en la tabla III.

Equipo	Dirección de Red
Asterisk Box	200.126.12.116 192.168.5.15
Teléfono IP	200.126.12.114
PC de prueba	200.126.12.109 192.168.5.10
Laptop 1	DHCP
Laptop 2	DHCP
Router SMesh / Router D-Link	200.126.12.120 192.168.5.19

Tabla III - Direcciones de Red asignadas.

Clientes Móviles

Los clientes son los generadores de tráfico en la red y a su vez quienes toman el papel del usuario en una situación real. Para las pruebas se utilizan clientes móviles y fijos. Los clientes móviles incluyen: dos Laptops para las pruebas y un teléfono Nokia E71, todos los clientes poseen una aplicación SIP con la capacidad de registrarse a la PBX y realizar y recibir llamadas. Dependiendo de la red a la cual se encuentran conectadas, cambian sus configuraciones de Red.

A continuación se detalla en la tabla IV las especificaciones de los clientes móviles:

Equipo	Dirección de Red
Laptop 1	HP Pavilion Athlon 2.0Ghz 2Gb Ram.
Laptop 2	Toshiba. Intel Atom 2.0Ghz 2GB Ram.

Tabla IV - Especificaciones clientes móviles.

Clientes Fijos

En cuanto a los clientes fijos, se utiliza una PC con una direcciOn IP pUblica y una privada para las pruebas relacionadas a perdida de paquetes detalladas mas adelante. Tambien se utiliza un telEfono IP que posee una direccion privada de red asociada a la respectiva direccion privada de la PBX. Las pruebas realizadas con el telEfono IP se detallan mas adelante.

Los Nodos

Los Nodos son los equipos utilizados como nodos Mesh o nodos de Acceso en el caso de la red ESPOL.

- **Meraki/Roofnet:** Nodos Meraki Outdoor. Antenas de 2dBi, dos puertos 10/100 Mbps PoE y procesador de 233 Mhz. Es Plug & Play: simplemente se conectan y adquieren la dirección vía DHCP. Deben estar conectados a Internet para funcionar, caso contrario la red no permite el tráfico de datos.
- **SMesh:** Dos Routers Linksys WRT54G-TM, con procesador de 200 Mhz. Un router WRT54G-L con procesador de 200Mhz. En ambos casos su OS basado en Linux, por lo que es compatible con SMesh.
- **ESPOL:** Enrutadores Cisco AIR-AP1131A6 y un AIR-AP1136AG. El segundo mucho más potente y es utilizado en la zona de Aulas FIEC.

En la tabla V se encuentran las especificaciones del telefono IP y la PC.

Equipo	Especificaciones
PC	Intel Core 2 Duo 2.0 Ghz 2 Gb RAM DDR3.
Teléfono IP	Grandstream.

Tabla V - Especificaciones clientes fijos.

Software utilizado.

El Software lo conforman los programas ó aplicaciones que se utilizan para realizar llamadas, realizar site survey y medir los parámetros de Calidad de Servicio.

Software para realizar llamadas.

Las aplicaciones encargadas de realizar las llamadas, asi como registrarse en la PBX se conocen como clientes SIP, pero con el fin de no crear ambiguedad con el hardware, se conocera a los clientes SIP como softphones.

El Nokia E71 posee un softphone que es capaz de conectarse a la PBX y realizar y recibir llamadas. Es una aplicacion incluida entre las aplicaciones predeterminadas del telefono y desarrollada por Nokia.

Las laptops y la PC tienen instalados un softphone llamado X-Lite. Posee las funcionalidades de un telefono IP, pero para efectos de las pruebas a realizarse es suficiente el hecho de recibir y realizar llamadas. La compania que desarrollo X-Lite se llama Counterpath .

Software para medir parametros de Calidad de Servicio.

El software dedicado a medir Calidad de Servicio es el software que censa los paquetes entrantes y salientes al hardware en cuestion y que tienen la finalidad de cuantificar los paquetes perdidos, asi como la latencia y jitter (parametros especificados en el capitulo 2.X). El software principal para realizar las pruebas es Wireshark, un sniffer que no solo censa paquetes entrantes y salientes, sino que entrega estadisticas y permite almacenar un archivo de texto tanto para el canal de entrada como el de salida.

No obstante, en pruebas preliminares para la solucion SMesh, se pudo verificar una incoherencia al terminar un recorrido: debido a la naturaleza de su arquitectura y funcionamiento, durante un handoff los nodos que atienden al cliente envian, durante un tiempo corto, paquetes duplicados se envian al cliente. Los detalles especificos del funcionamiento de SMesh se puede encontrar en el Capitulo 1.X.

El problema fundamental es la incapacidad de Wireshark de brindar una opción de reconocer paquetes UDP duplicados y no contarlos en el análisis de streaming posterior a la prueba, por lo que no existe una

forma de reconocer una secuencia de paquetes y, por tanto, la utilidad de este aplicativo resulta ser nula para el análisis de paquetes perdidos.

Para resolver este problema, se desarrolló dos programas para resolver el problema de los paquetes perdidos. Para el transmisor se escribió un programa en Python que envía paquetes de 160 bytes cada 20 milisegundos, con lo cual se simula una conversación VoIP de 64 kbps. Del lado del receptor se escribió un programa en Java que elimina los duplicados y determina los paquetes perdidos. Del lado del transmisor, el programa arma los paquetes de tal forma que siga una secuencia numérica en los datos. La secuencia va desde el cero hasta el número de paquetes enviados totales. Para los experimentos se trabajó con 5000 paquetes enviados en el recorrido. El programa llena los datos con la secuencia numérica, seguida de bytes de relleno para completar 160 bytes en los datos. El programa de Java recibe los paquetes y, luego de un tiempo determinado, realiza el censo de los paquetes duplicados y los perdidos gracias a la secuencia numérica seguida. Es un método bastante sencillo, pero efectivo para este tipo de pruebas en los que los que la red presenta dificultades para medir paquetes perdidos.

El código del programa principal se encuentra incluído en el Anexos.

Wireshark por sí solo no brinda gráficos muy exactos y suele tener fallos al graficar, por lo cual se desarrolló un Software en Java que organiza los datos en formato CVS de Wireshark y crea archivos de texto con un CVS más limpio. Adicionalmente, el programa se encarga asimismo de realizar todos los cálculos.

Por otra parte, se desarrolló un script sencillo en MATLAB que grafica el contenido de dichos documentos.

La modularización fue importante por cuanto una parte del software se encargó de organizar y cuantificar los datos, mientras que el otro fue utilizado sólo para graficar.

3.1.3. Parámetros de medición.

Los parámetros de medición son todos aquellos datos que contribuyan a una toma de decisión sobre la mejor solución. Dicha decisión se basa en parámetros de Calidad de Servicio (detallados en el Capítulo 2) y son: Jitter, Paquetes Perdidos, Latencia (Delay) y Ancho de Banda (Bandwidth). Los datos antes mencionados serán tomados durante las pruebas utilizando las herramientas de medición mencionadas en 3.1.1.

Adicionalmente, se plantea la medición de MOS como método alternativo a mediciones subjetvas. Como se indica en el capítulo 2, las pruebas que incluyen mediciones subjetivas son importantes para productos finales y son más comunmente utilizadas para establecer la calidad de servicio en un producto desde el punto de vista del consumidor final. A pesar que un objetivo directo del presente trabajo no es presentar un producto final que deba ser evaluado con dicho método de satisfacción de usuario, sí le agrega valor al estudio de varias soluciones a Voz sobre WLAN.

3.1.4. Soluciones Consideradas

El objetivo de este trabajo es probar la efectividad de las soluciones dentro de la las instalaciones de la FIEC. Las soluciones consideradas para las pruebas incluirán una implementación completa en las instalaciones de la FIEC descritas anteriormente, tomando en cuenta que las pruebas:

Son realizadas a lo largo de un recorrido que empieza en el antiguo laboratorio de telecomunicaciones y termina en las inmediaciones del bar FIEC.

Para las implementaciones con Redes Wireless Mesh, los nodos tendrán una ubicación predeterminada mostradas en el gráfico 3.1. Los nodos de las redes de la ESPOL tendrán ubicaciones diferentes, mostrados en el gráfico.

- Utilizarán el mismo hardware que incluye: la PBX con Asterisk, un teléfono IP y una red LAN privada.
- Utilizarán el mismo software de medición de Calidad de Servicio: Wireshark para medir: Jitter, Latencia, Ancho de Banda y Paquetes perdidos, a excepción de SMesh que utilizará programas creados para las pruebas de paquetes perdidos.
- La conexión de la red Mesh a la LAN cambia respecto de la solución por detalles a explicados más adelante.

Las soluciones consideradas son las siguientes:

Meraki

Se considera la solución Meraki como la representante a una red Mesh convencional. De acuerdo a mencionado previamente en el capítulo 1, una red Mesh creada con Meraki permite conectar y usar el equipo de inmediato (plug and play), luego de que la red se conecte con Meraki

vía Internet. En cuanto a roaming, las redes Roofnet (Meraki) no ofrecen un plan específico de handoffs, por lo que es un candidato idóneo para el análisis comparativo en la presente Tesis.

Es necesario colocar un router como elemento adicional para conectar la PBX con el Router Gateway Meraki, debido a que éste último dispone únicamente de una conexión LAN, que le sirve de conexión a internet (indispensable para que el router funcione). El esquema final se encuentra detallado en la figura 3.1.

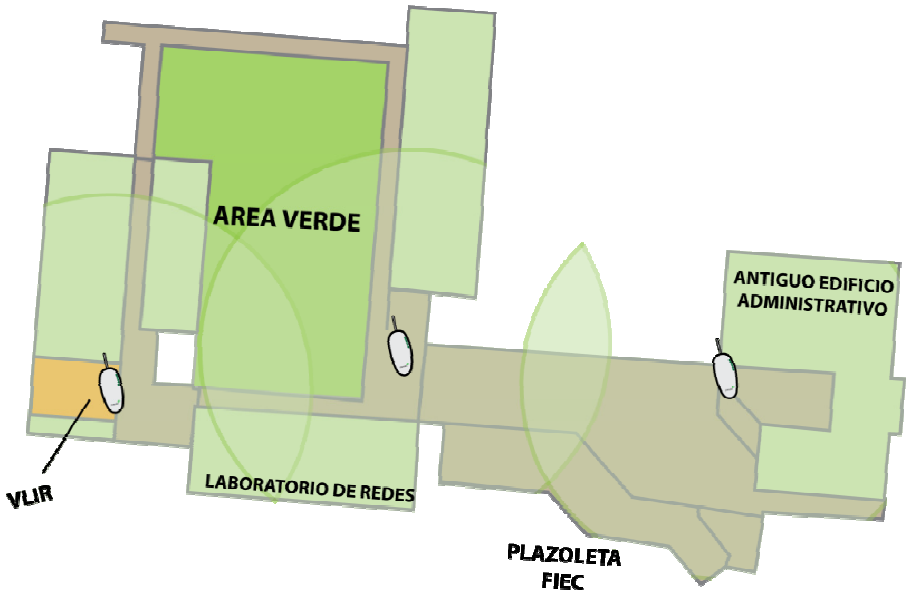

Figura 3-1 - Ubicación de Routers Meraki

SMesh

Se considera la solución SMesh como la solución a los problemas experimentados en la comunicación de VoIP over WLAN y Wireless Mesh Networks, como se presenta en la Tesis actual. SMesh contará con un software programado especialmente para medir paquetes perdidos. En la figura 3.2 se muestra cómo se distribuyen los nodos SMesh para las pruebas.

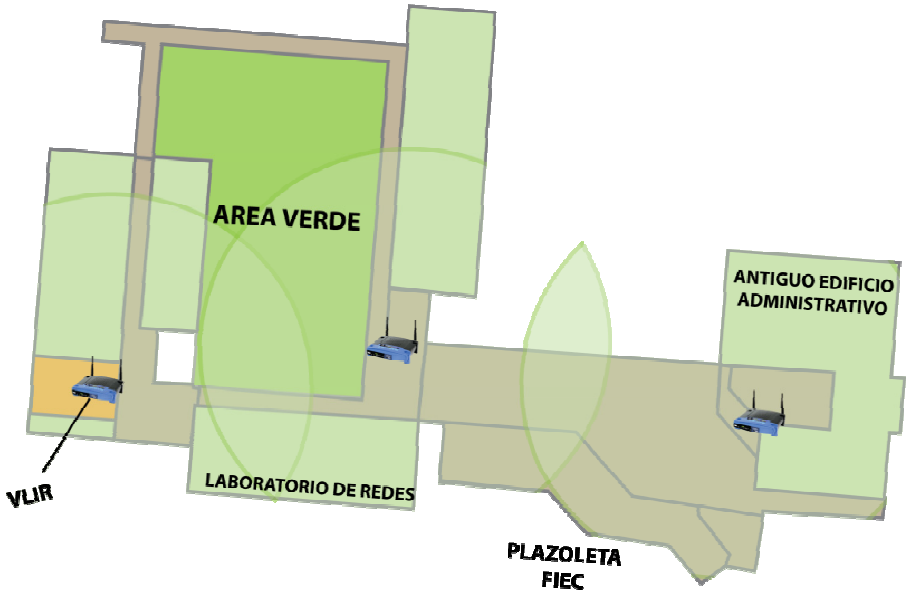

Figura 3-2– Ubicación de Routers SMesh

Red ESPOL

Los análisis correspondientes a la Red WLAN ESPOL no serán sometidos a una comparación directa puesto que el objetivo de la presente Tesis es contrastar dos soluciones VoIP en Wireless Mesh

Networks. Se incluye la red ESPOL en las pruebas para dar una primicia a un futuro estudio de factibilidad de la implementación de una red VoWLAN en la ESPOL, presentando una comparación entre diferentes soluciones y topologías de Red. La ubicación de los nodos se presenta en la figura 3.3.

Figura 3-3– Ubicación y cobertura aproximada de los nodos ESPOL

3.2. Costos

Para una implementación de una Red VoIP es siempre necesario realizar un análisis de precios. Es un factor importante dentro de una toma de decisión final. Por ello, en la presente tesis se ha considerado

incluir un detalle de precios para implementar el Testbed. En la tabla VI se encuentran detallados el costo aproximado para el caso de la Red Meraki, mientras que en la tabla VII se encuentra detallado el costo aproximado de los nodos.

Equipo	Precio
Cables Ethernet. (5)	$15.00
PC (Asterisk PBX).	$500.00
Grandstream Teléfono IP	$95.00
D-Link Router	$45.00
Laptop	$400.00
Total	$655.00 / $1055 con laptop

Tabla VI - Precio aproximado de Equipos

Router	Precio
Routers ESPOL (Aironet)	$496.7.00
Router Meraki.	$199.00
Routers SMesh (WRT54G)	$70.00

Tabla VII - Comparativa de costo de nodos.

Como se puede observar, la solución más barata es SMesh, le sigue Meraki y por último la solución más cara es implementar con routers Aironet de Cisco para la red ESPOL.

3.3. Descripción de los experimentos.

El Testbed implementado con el fin de negar o demostrar la hipótesis planteada en el capítulo 1, constituye un conjunto de características mencionadas en el presente capítulo que van a ser especificadas en esta sección.

Objetivos de los Experimentos

- Corroborar o descartar la hipótesis planteada "La Calidad de Servicio en Voz sobre Redes Inalámbricas se ve mejorada con el uso de SMesh en comparación con el uso de otras redes tradicionales Wireless Mesh y Wireless LAN tradicionales dentro de instalaciones de la FIEC".
- Presentar datos correspondientes a calidad de servicio en la comunicación de voz sobre WLAN dentro de un área específica de la FIEC, que sirvan de apoyo y motivación para futuras pruebas que viabilicen la implementación de VoWLAN en la ESPOL.
- Utilizar los conocimientos adquiridos durante la carrera para realizar pruebas de calidad de servicio en comunicaciones de voz sobre WLAN.

- Comparar soluciones de VoWLAN y presentar la más adecuada para el ambiente FIEC - ESPOL donde se llevan a cabo las pruebas.

Descripción de las Pruebas

Como se ha mencionado a lo largo del presente capítulo, los experimentos varían de acuerdo a la solución a tratar. No obstante, existen varias constantes en el desarrollo de los experimentos, sin importar la solución:

- Durante todas las pruebas, se realizará el mismo recorrido mostrado en la figura 3.4.

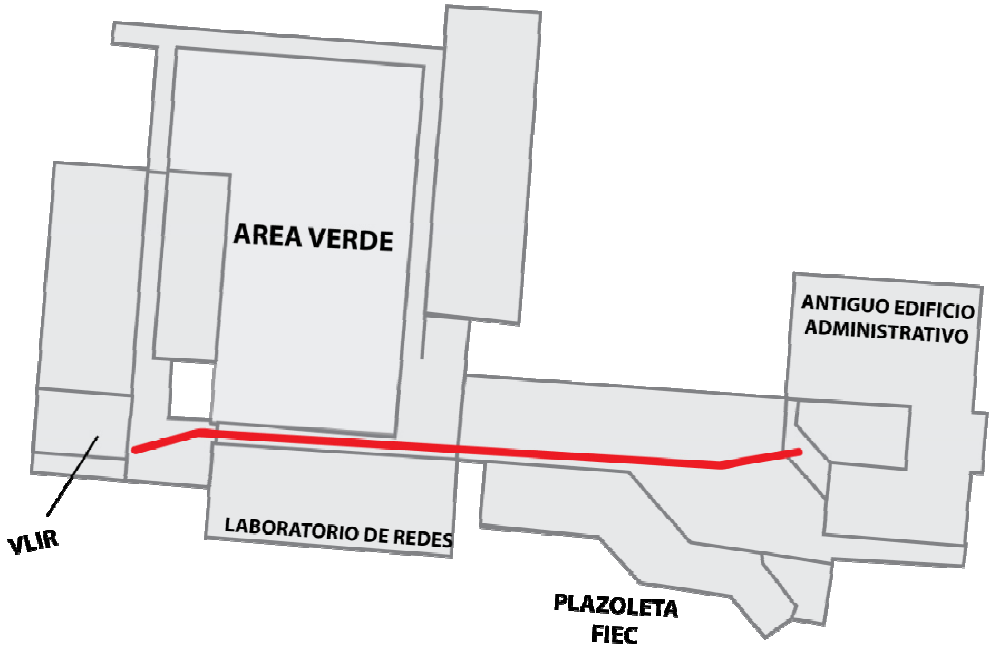

Figura 3-4 – Recorrido en los experimentos.

- El recorrido en las pruebas tendrá una duración promedio de 1 minuto y medio.

- Para todas las pruebas, se utilizará Wireshark como herramienta de medición de calidad de servicio, específicamente latencia, jitter, paquetes perdidos y ancho de banda. Sólo la solución SMesh tendrá un software diferente para la medición de paquetes perdidos.
- En todas las pruebas se utilizará un softphone en el cliente móvil, que será una laptop, y un teléfono IP. La única prueba que no

contará con ambos aplicativos serán las prueba de paquetes perdidos de SMesh.

- En todas las pruebas se utilizará una PBX opensource llamada Asterisk como administrador de llamadas.
- En todas las pruebas existirá una LAN privada asociada a la red WLAN. La excepción es las pruebas con WLAN ESPOL que tiene su propia red que se conecta mediante la dirección pública a la PBX open source.

Estos son los detalles específicos por solución:

Meraki

El nodo gateway Meraki estará conectado a un router, al cual también se encuentra conectada la PBX Asterisk, ambos con una direcciones privadas.

El esquema de la red completa se muestra en la figura 3.5.

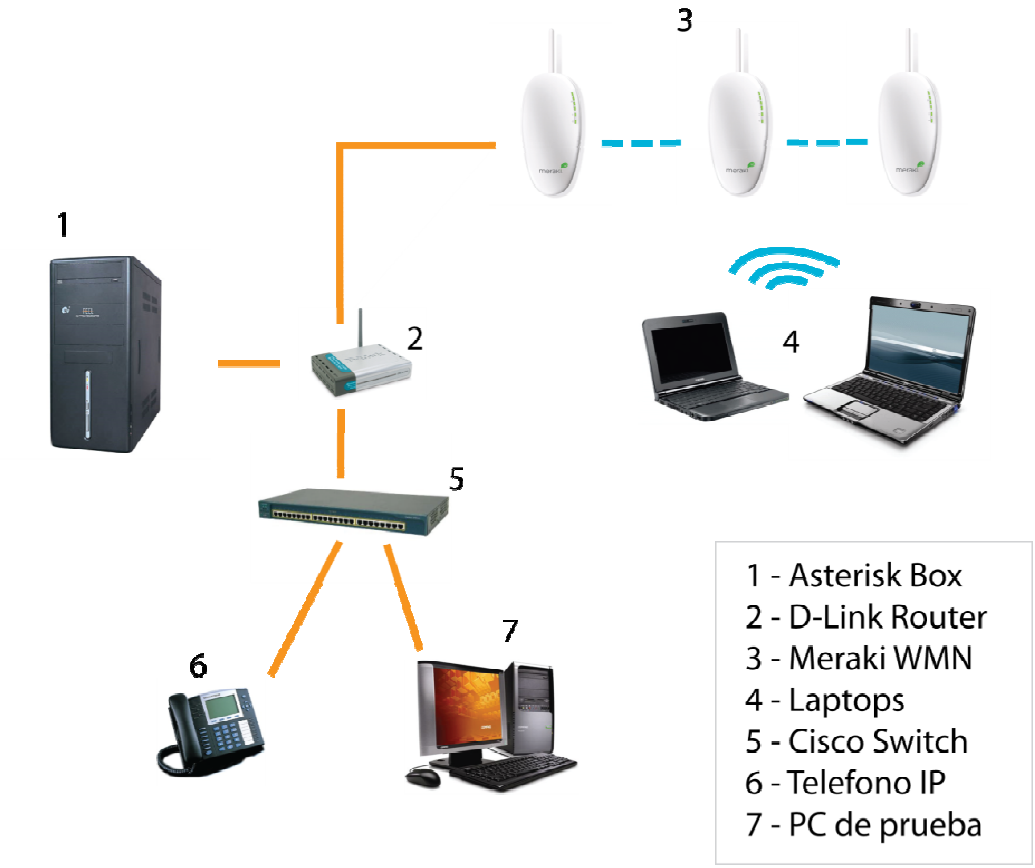

Figura 3-5 – Esquema de red para pruebas con Meraki.

SMesh

La prueba de pérdida de paquetes será realizada con software programado en Python y Java para emisión y recepción de paquetes, respectivamente.

El esquema de la red completa se muestra en la figura 3.6.

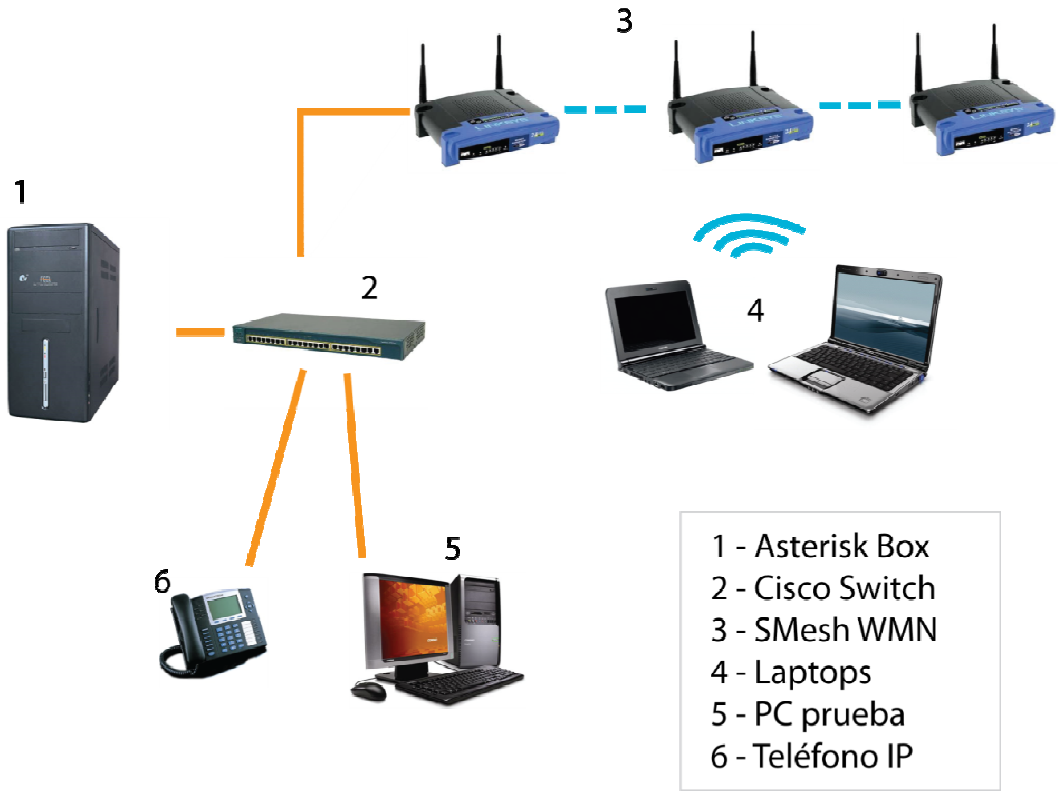

Figura 3-6– Esquema de red para pruebas con SMesh.

CAPÍTULO 4

4. ANALISIS COMPARATIVO DE LA IMPLEMENTACION DE VOZ SOBRE UNA RED WIRELESS MESH CON SOLUCIONES COMUNES VERSUS EL USO DE SMESH MEDIANTE EL USO DE UN TESTBED

4.1. Evaluación de los Resultados en términos de QoS subjetiva.

En el transcurso de las pruebas de QoS subjetiva – MOS, fue evidente la falta de criterio técnico que tienen muchos usuarios de prueba al escuchar durante el recorrido el audio que escuchaban. Debido a ello, los resultados para ambas pruebas resultó ser bastante aproximado. Ambas redes, luego de una prueba rápida de experiencia de usuario por

parte de algunos voluntarios resultó aproximado a 4 sobre 5. No obstante, las diferencias entre ambas redes no resultaron quedar claras por cuanto los evaluados fueron diferentes para cada ocasión.

Es por ello que se procedió a revisar el audio de las pruebas. Gracias a que la canción era conocida, se pudo apreciar los puntos en los que el audio se escuchaba muy adelantado o muy entrecortado.

Por un lado, la red Meraki obtuvo un promedio de 3 puntos de fallo en los segundos 38, 55 y 70 aproximadamente. Por otra parte, SMesh obtuvo ligeros problemas de audio evidenciados en los segundos 55 únicamente con un promedio de 1 error por canción. ESPOL por su parte obtuvo de 4 a 5 errores evidentes en el audio.

Esto es favorable para SMesh por cuanto la percepción final del audio tuvo una nitidez mayor que en el caso de Meraki y de ESPOL.

4.2. Evaluación de los Resultados en términos de QoS objetiva.

Meraki

Delay

La figura 4.1 muestra el Delay o Latencia promedio de retorno para el caso de la red Meraki. Como se puede apreciar, el Delay Medio se encuentra ubicado en 21.2 milisegundos, con un máximo de 24.15 y un mínimo de 19.96 milisegundos.

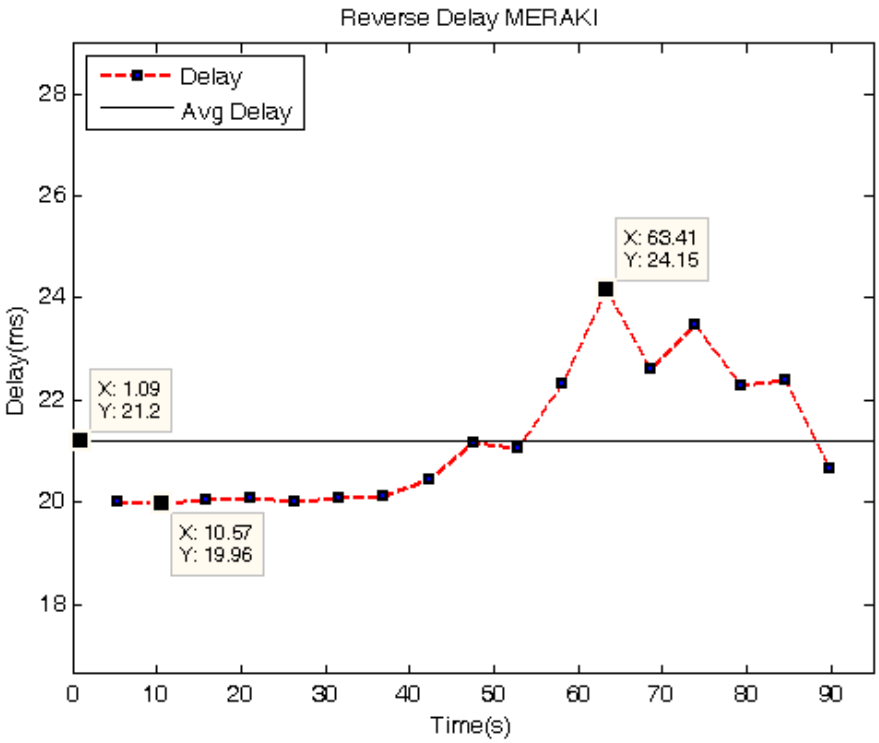

Figura 4-1 – Delay de Reversa en la red Meraki

En la figura 4.2 se muestra la probabilidad de Delay en la Red Meraki.

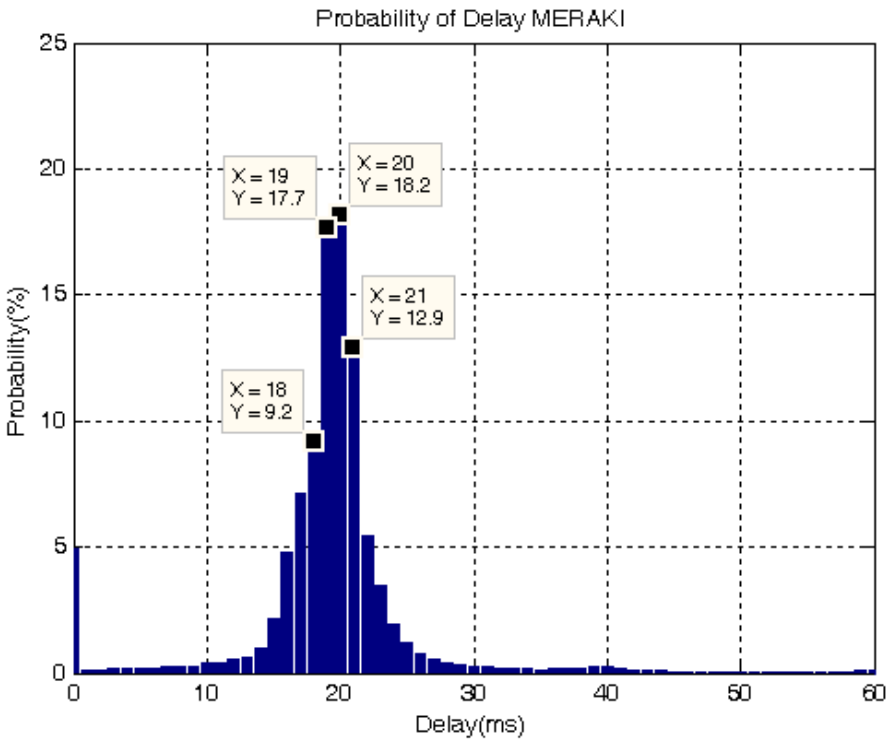

Figura 4-2 – Probabilidad de Delay en red Meraki.

Como se puede apreciar, la mayor probabilidad de Retardo la comparten los paquetes que lleguen con un retardo de 19 y 20 milisegundos con 17.7% y 18.2% respectivamente. En otras palabras, un paquete tiene una probabilidad aproximada de 17.7% de llegar con 19 milisegundos de retardo y de 18.2% de probabilidad de llegar con 20 segundos de retardo.

Los resultados de las pruebas de Delay para la red Meraki son favorables por cuanto en promedio la red presenta un retardo de paquetes aceptable y dentro del límite óptimo de 150 milisegundos.

La Tabla VIII muestra el número de paquetes con mayores que 100, 150, 400 y 800 milisegundos y los paquetes que se encuentran dentro de 100 y 150 milisegundos así como el porcentaje que representan dichos números frente al total de paquetes cuyo retraso fue mayor a 150 milisegundos.

Límite	Paquetes	Porcentaje
> 100 ms	354	100.00%
> 150 ms	273	77.10%
> 400 ms	141	39.83%
> 800 ms	1	0.28%

Tabla VIII - Número de paquetes cuyo delay fue mayor a 100, 150, 400 y 800 milisegundos red Meraki.

Se ha propuesto un límite de 100 milisegundos especial para analizar aquellos paquetes que exceden una cuota 5 veces superior a la media de 20 milisegundos.

Como es posible observar de la VIII, el 77.1% de los paquetes (es decir, más de tres cuartos del total) que fueron mayores a 100 milisegundos fueron a su vez mayores a 150 milisegundos. Por otra parte, el 39.8% de los paquetes cuyo retraso fue mayor que 100 milisegundos fue también mayor a 400 milisegundos.

De 71 mil paquetes en total acumulados de todas las pruebas realizadas, a penas 354 llegaron con un retraso mayor a 100 milisegundos y 273 con un retraso mayor a 150 milisegundos. Eso representa mucho menos del 1%.

Jitter

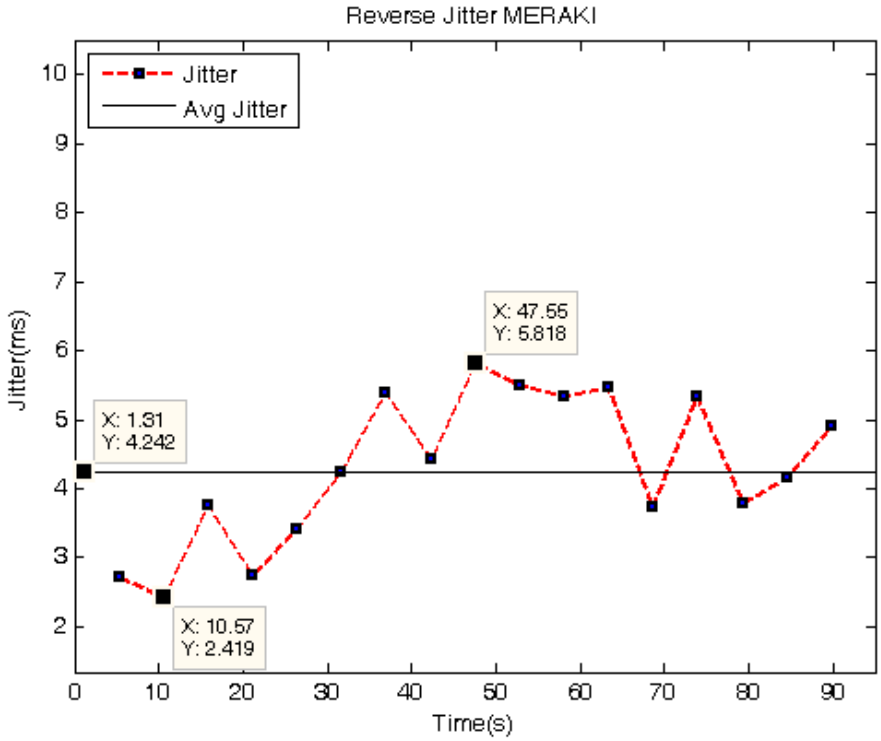

Figura 4-3– Jitter promedio en red Meraki.

Como se puede observar en la Figura 4.3, el Jitter promedio se ubica en 4.2 milisegundos, con un máximo de 5.8 y un mínimo de 2.4 milisegundos. Esto es positivo por cuanto se encuentra dentro del límite de 100 ms aceptado por la ITU.

Packet Loss

Las pruebas de pérdida de paquetes mostraron un promedio de 30 paquetes perdidos por cada 5000. Eso representa mucho menos del 1%, por lo que se puede decir que está dentro de los parámetros aceptables por la ITU.

Ancho de Banda

La Figura 4.4 corresponde al gráfico de Ancho de Banda promedio resultante de las pruebas con Meraki. Como se puede observar, el ancho de banda promedio fue de 77.4 kbps con un máximo de 81.1 y un mínimo de 69.8 kbps. Un ancho de banda por debajo de los 80 kbps que necesita el códec G.711 implica una recepción pobre de voz. Esto, por supuesto, no quiere decir que el Testbed de Meraki no sea idóneo para realizar las comparaciones con las otras redes, sino que provee de información adicional acerca de la calidad de comunicación brindada por la red.

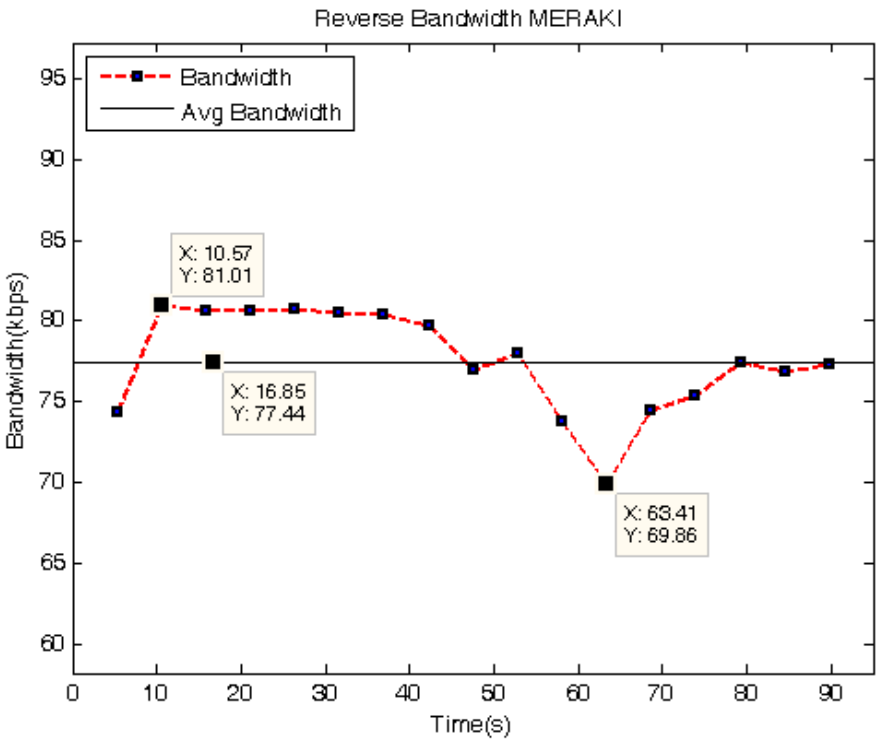

Figura 4-4 – ancho de banda de reversa para Meraki.

Pruebas de Tráfico

La Tabla IX muestra los valores correspondientes a el número de llamadas respecto y el porcentaje de bloqueo.

Saltos	Llamadas
0	675
1	337.5
2	168.75

Tabla IX - Número máximo teórico de llamadas por salto Meraki.

Llamadas	% Bloqueo
80	8.00%
85	8.60%
90	11.00%
100	14.00%
550	21.30%

Tabla X - Porcentaje de bloqueo de llamadas Meraki. 0 saltos.

Llamadas	% Bloqueo
80	6.30%
85	9.40%
90	11.00%
168	18.50%

Tabla XI - Porcentaje de bloqueo de llamadas Meraki. 1 saltos.

Llamadas	% Bloqueo
50	9.10%
55	11.70%
168	18.50%

Tabla XII - Porcentaje de bloqueo de llamadas Meraki. 2 saltos.

Las tablas X, XI y XII muestran el porcentaje de bloqueo de llamadas para los saltos cero, uno y dos respectivamente.

Salto	Llamadas
0	85
1	85
2	50

Tabla XIII - Número recomendado de llamadas por salto red Meraki.

La Tabla XIII resume el número (máximo) de llamadas recomendadas por salto antes de llegar al 10% de porcentaje de bloqueo de llamadas. Es posible resumir que el número recomendado de llamadas que evite el bloqueo de llamadas de más del 10% sea de 50 llamadas concurrentes para la red Meraki.

SMesh

Delay

El gráfico de Delay promedio de reversa para SMesh se puede encontrar en la figura 4.5. La media del Delay promedio se encuentra en 19.79 milisegundos, mientras que el máximo se ubica en 20.22 ms y el mínimo en 19.36 milisegundos.

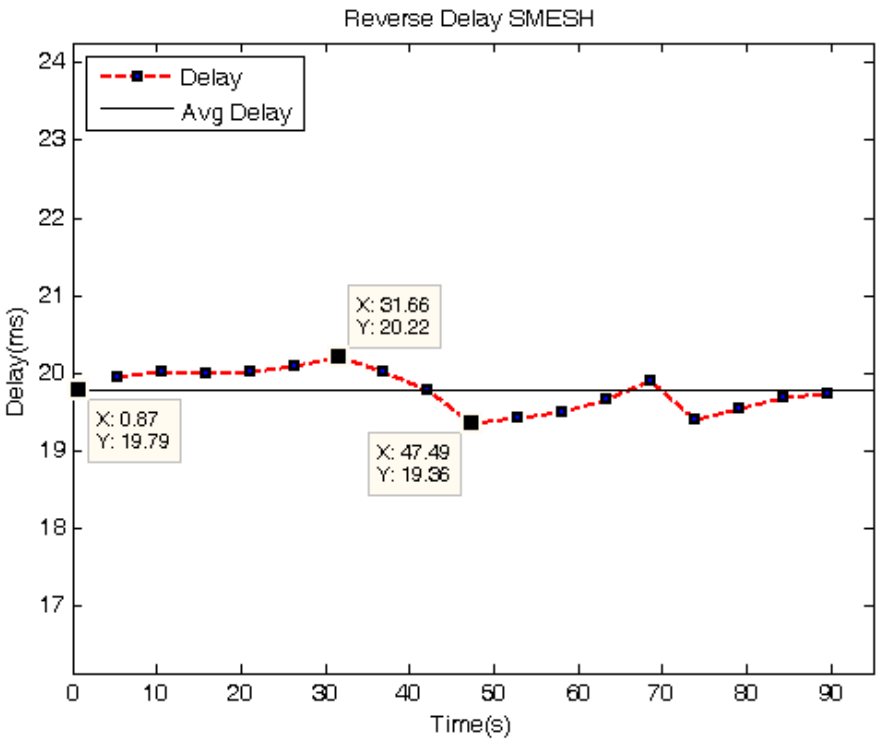

Figura 4-5– Delay de Reversa para red SMesh.

Esto ubica a SMesh muy por debajo del límite aceptable de 150 milisegundos, por lo cual es posible tomar en consideración los resultados de Retardo para las comparaciones posteriores.

La figura 4.6 muestra la probabilidad de Delay para la red SMesh. Como se puede observar, existe un 20.7% de probabilidad para que un paquete en 20 milisegundos de retraso, seguida de un 20.1% de probabilidad de que llegue con 19 milisegundos de retraso, siendo estos últimos dos valores de retardo los que mayor probabilidad obtienen de las pruebas.

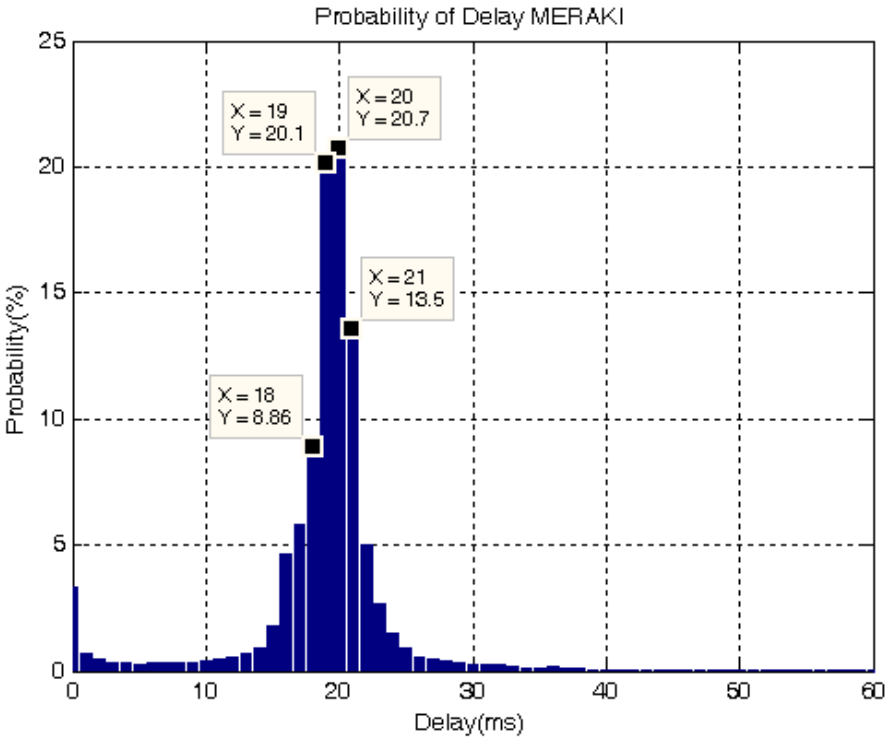

Figura 4-6– Gráfico de probabilidad de Delay para red SMesh.

La Tabla XIV muestra el número de paquetes con mayores que 100, 150, 400 y 800 milisegundos y los paquetes que se encuentran dentro de 100 y 150 milisegundos así como el porcentaje que representan dichos números frente al total de paquetes cuyo retraso fue mayor a 150 milisegundos.

Límite	Paquetes	Porcentaje
> 100 ms	156	100.00%
> 150 ms	88	56.41%
> 400 ms	51	32.69%
> 800 ms	1	0.64%

Tabla XIV - Número de paquetes cuyo delay fue mayor a 100, 150, 400 y 800 milisegundos, red SMesh.

Se ha propuesto un límite de 100 milisegundos especial para analizar aquellos paquetes que exceden una cuota 5 veces superior a la media de 20 milisegundos.

Como es posible observar de la Tabla XIV, el 56.4% de los paquetes (es decir, un poco más de la mitad) que fueron mayores a 100 milisegundos fueron a su vez mayores a 150 milisegundos. Por otra parte, aproximadamente la tercera parte de los paquetes cuyo retraso fue mayor que 100 milisegundos fue también mayor a 400 milisegundos.

De 71 mil paquetes en total acumulados de todas las pruebas realizadas, a penas 156 llegaron con un retraso mayor a 100 milisegundos y 88 con un retraso mayor a 150 milisegundos. Eso representa mucho menos del 1%.

Jitter

En la figura 4.7 se muestra el Jitter de reversa promedio para la red SMesh. La media general del Jitter promedio para la red SMesh se encuentra en 3.178 milisegundos, con un máximo de 4.63 milisegundos y un mínimo de 2.1 milisegundos. Esto es positivo para el análisis posterior dado que se encuentra por debajo de lo recomendado para el Jitter para tráfico en tiempo real.

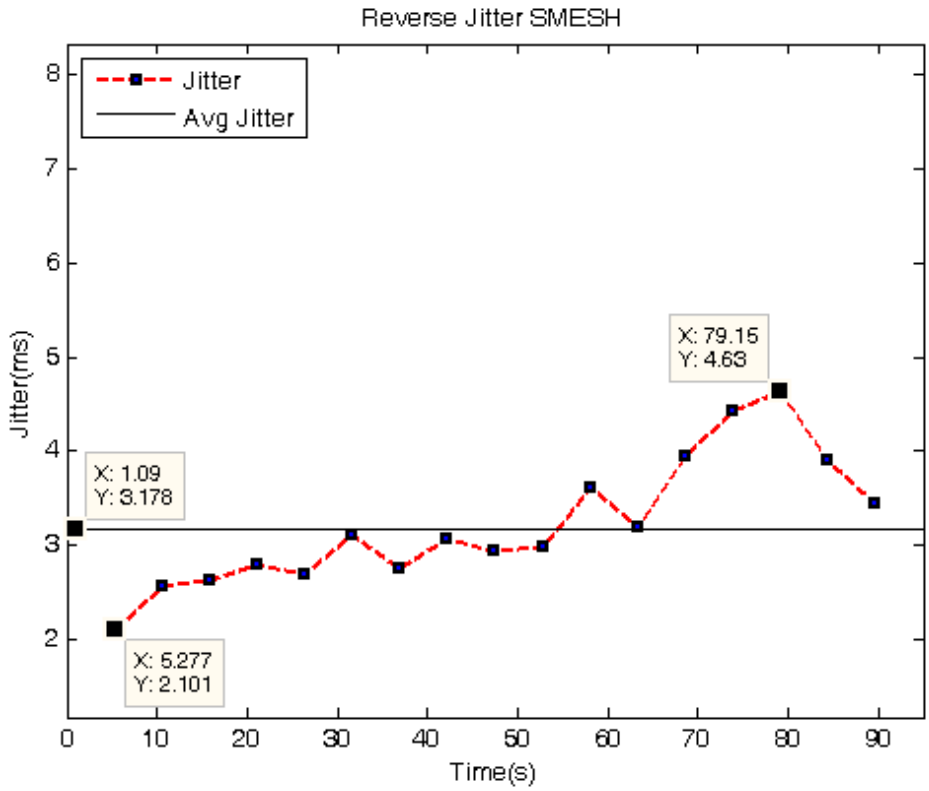

Figura 4-7 – Jitter de reversa para red SMesh.

Packet Loss

La media del packet loss se ubicó en 19 paquetes perdidos por cada 5000 paquetes enviados. Esto ubica a SMesh dentro de una red segura para el tráfico de voz sobre IP, puesto que la tasa de paquetes perdidos se encuentra muy por debajo del 1%.

Ancho de Banda

La Figura 4.8 ilustra el ancho de banda medido a lo largo de la prueba con la red SMesh. El gráfico muestra una media de 82.29 kbps, mientras que a su vez se puede apreciar un máximo de 85.84 y un mínimo de 74.97 kbps. Si bien es cierto que el exceso de ancho de banda no es una influencia negativa directa en el rendimiento de la comunicación, el exceso de uso de ancho de banda en la red podría implicar menos ancho de banda disponible para otras llamadas concurrentes. No obstante, es importante aclarar que para en este caso el exceso de ancho de banda no es especialmente significativo.

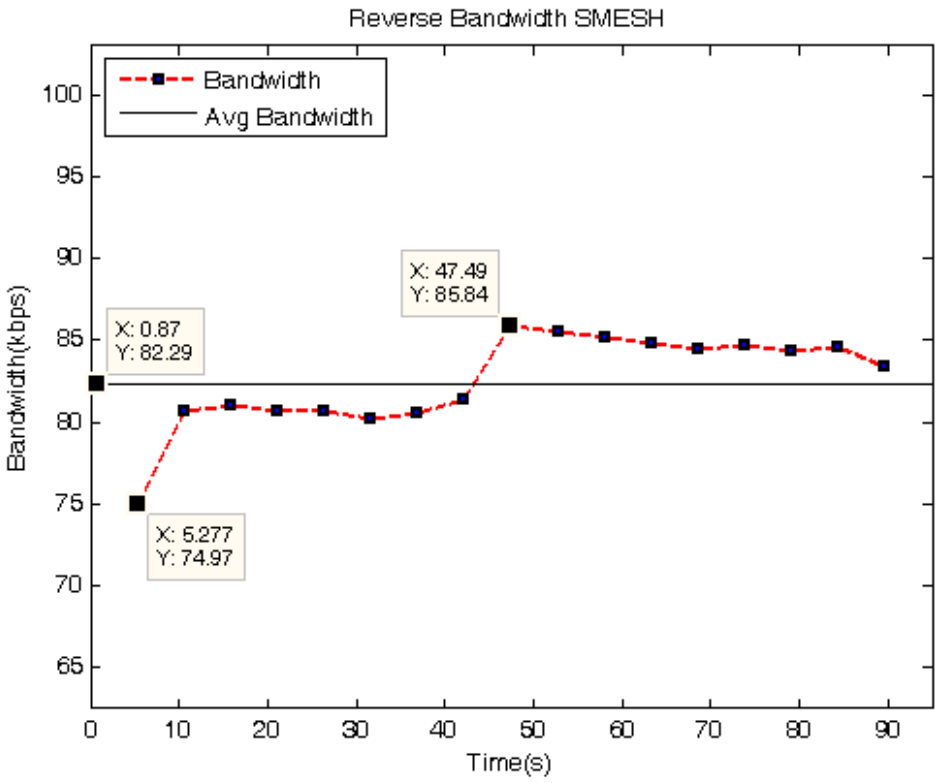

Figura 4-8 – Ancho de banda en la red SMesh.

Pruebas de Tráfico

La Tabla XV muestra el número teórico de llamadas bloqueadas por salto. Esto se obtuvo gracias al cálculo siguiente: el máximo throughput que ofrecen la interfaz inalámbrica es de 11 Mbps en el primer nodo, mientras que para el segundo y el tercero son 5.5 Mbps y 2.75 Mbps respectivamente, de acuerdo con el principio que supone el corte de la mitad del throughput por salto en una red inalámbrica. Los valores para los nodo 3 nodos son 135, 68 y 34 llamadas máximas a 80 kbps. No obstante, esto no implica necesariamente que dichos valores tengan

que ser un límite, dado que el ancho de banda disponible por llamada será inferior. Es por ello que se optó por calcular el punto en el que se excede del 10% en la probabilidad de bloquedo de llamadas.

Saltos	Llamadas
0	135.5
1	68.8
2	34.3

Tabla XV - Número máximo teórico de llamadas por salto SMesh.

Llamadas	% Bloqueo
90	0.00%
100	4.00%
105	7.50%
110	11.82%
140	38.57%
145	40.69%

Tabla XVI - Porcentaje de bloqueo de llamadas SMesh. 0 saltos.

Llamadas	% Bloqueo
55	5.47%
60	16.67%
65	27.69%
68	29.41%

Tabla XVII - Porcentaje de bloqueo de llamadas SMesh. 1 saltos.

Llamadas	% Bloqueo
30	0.00%
34	8.82%
35	11.43%
40	27.50%
50	46.00%

Tabla XVIII - Porcentaje de bloqueo de llamadas SMesh. 2 saltos.

Las tablas XVI, XVII y XVIII muestran el porcentaje de bloqueo de llamadas para los saltos cero, uno y dos respectivamente.

Salto	Llamadas
0	105
1	55
2	30

Tabla XIX– Número recomendado de llamadas por salto red SMesh.

La Tabla XIX resume el número (máximo) de llamadas recomendadas por salto antes de llegar al 10% de porcentaje de bloqueo de llamadas. Es posible resumir que el número recomendado de llamadas que evite el bloqueo de llamadas de más del 10% sea de 30 llamadas concurrentes para la red SMesh.

Red ESPOL

Delay

La Figura 4.9 muestra el delay de reversa en la red ESPOL sin normalizar. Como se puede apreciar, al inicio de las pruebas se presentaba una secuencia de paquetes con un retardo superior a 200 milisegundos. De igual forma, cerca del final del recorrido se pudo apreciar un incremento significativo, aunque no superior a 150 milisegundos, de retardo en el arribo de paquetes. El gráfico de retardo muestra una media de 43.74 milisegundos, mientras que registra un mínimo de 14.35 milisegundos y un máximo de 203.3 milisegundos.

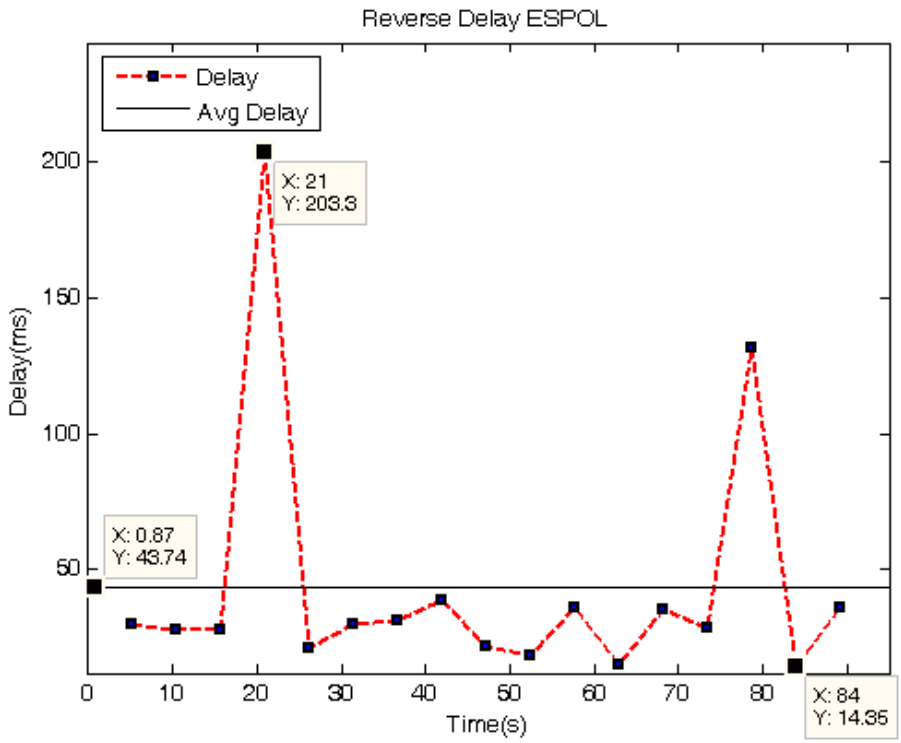

Figura 4-9 – Gráfico sin normalizar de Delay reverso para red ESPOL.

Si bien es cierto, estos datos no representan un mal desempeño en la red para el Delay en la comunicación de voz sobre IP; no obstante, sí demuestra un desempeño bastante irregular y poco confiable para la zona en la cual se realizaron las pruebas.

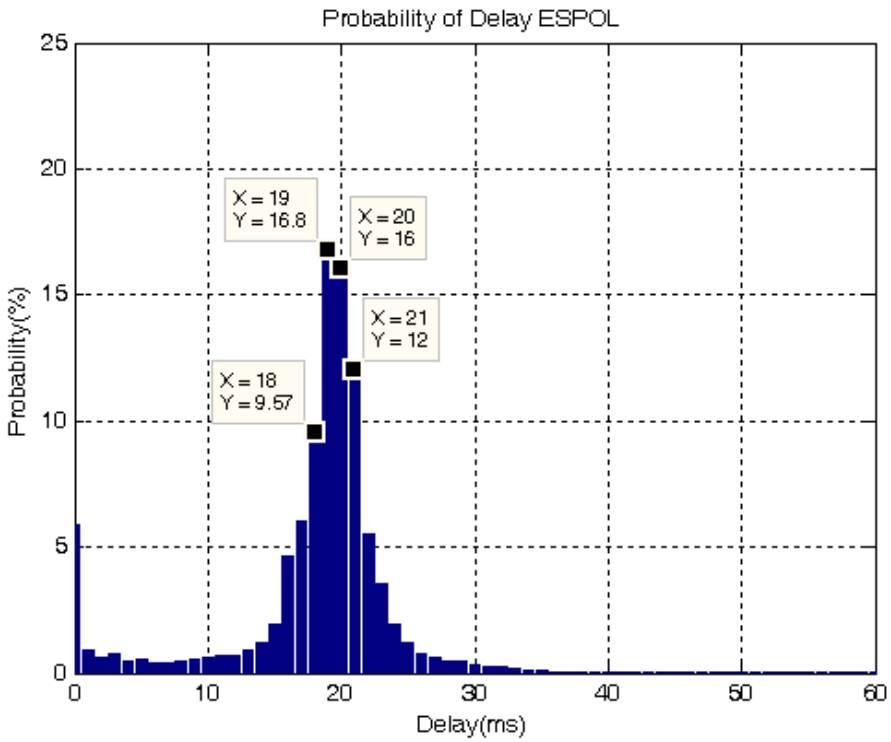

Figura 4-10 - Probabilida de Delay en red ESPOL.

No obstante, como muestra la figura, en general la red ESPOL presenta una probabilidad de Delay bastante cercana a los 20 milisegundos: un 19% de probabilidad para 19 milisegundos y una probabilidad de 16% para un arribo con 20 milisegundos de retardo. Esto demuestra que es posible mantener una conversación de voz utilizando la red ESPOL, teniendo la mayor probabilidad de arribo de paquetes cercanos a 20 milisegundos.

Es necesario destacar la diferencia entre los resultados de ambas gráficas. Por un lado, la Figura 4.10 que muestra la probabilidad de

retardo por paquete demuestra que la red cumple con los requerimientos mínimos, brindando una probabilidad máxima para paquetes que lleguen cerca de los 20 milisegundos, mientras que por otro lado, la Figura 4.9 que muestra el Delay promedio de reversa indica los bruscos cambios que se pueden presentar en la red ESPOL y, por tanto, es posible esperar un gran número de interferencias y molestias en la comunicación de voz sobre IP durante el recorrido.

La Tabla XX muestra el número de paquetes con mayores que 100, 150, 400 y 800 milisegundos y los paquetes que se encuentran dentro de 100 y 150 milisegundos así como el porcentaje que representan dichos números frente al total de paquetes cuyo retraso fue mayor a 150 milisegundos.

Límite	Paquetes	Porcentaje
> 100 ms	400	100.00%
> 150 ms	318	79.50%
> 400 ms	45	11.25%
> 800 ms	30	7.50%

Tabla XX - Número de paquetes cuyo delay fue mayor a 100, 150, 400 y 800 milisegundos red ESPOL.

Como es posible observar de la Tabla XX, el 79.5% de los paquetes que fueron mayores a 100 milisegundos fueron a su vez mayores a 150

milisegundos. Por otra parte, el 11.25% de los paquetes cuyo retraso fue mayor que 100 milisegundos fue también mayor a 400 milisegundos.

Cabe recalcar que la red ESPOL obtuvo un número significativo de paquetes mayores a 1 segundo. 30 paquetes llegaron con un retraso excesivamente alto.

Jitter

Como es posible apreciar en la Figura 4.11, existe un exceso de Jitter presente en la red ESPOL dentro del recorrido realizado en las pruebas alrededor de los 26 segundos con un valor de Jitter de 110.2 milisegundos, siendo éste el máximo en la gráfica, contrastando con un mínimo de 5.25 milisegundos. El promedio de Jitter se encuentra en 41.97 milisegundos.

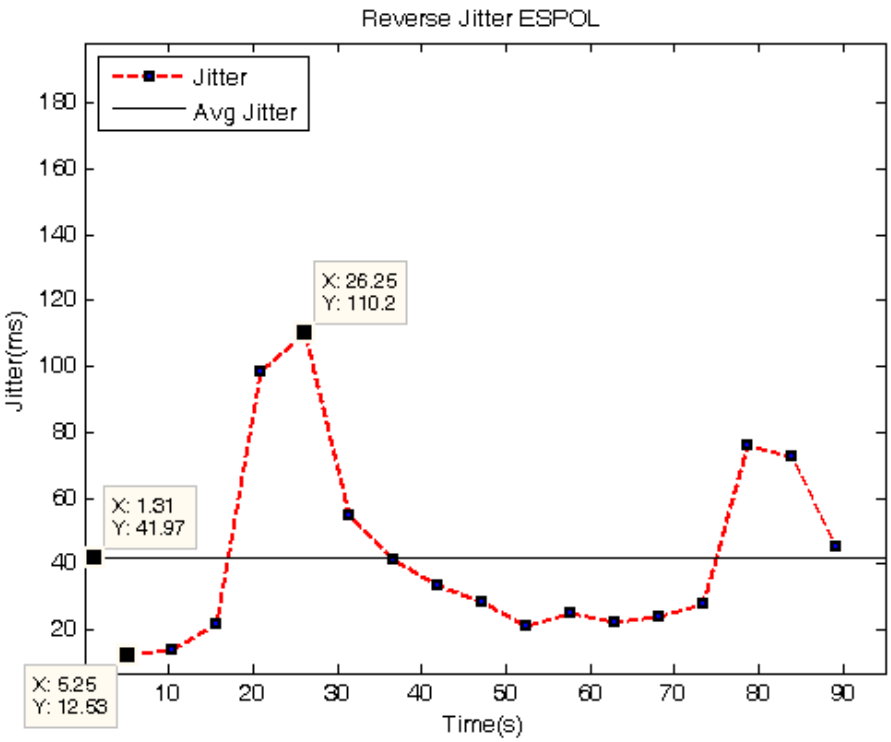

Figura 4-11– Gráfico de Jitter de reversa para red ESPOL.

Siendo el Jitter una variación del retardo en la red, podemos constatar que los grandes cambios del Jitter en la Figura 4.11 corresponden a los cambios vistos en la Figura 4.9.

Cabe acotar que en el tramo en el que se presentó un valor de Jitter mayor a 100 milisegundos, valor límite permitido antes de experimentar una degradación en la calidad de la conversación. No obstante, para el estudio no fue posible cambiar de posición los puntos de acceso a fin de mejorar los valores antes mencionados, por lo que los datos mostrados serán los utilizados para realizar la comparación adicional.

Packet Loss

Debido a que la red ESPOL bloquea puertos, no fue posible realizar la prueba con el software desarrollado, puesto que necesita utilizar un puerto no convencional.

Por otra parte, Wireshark arrojó porcentajes muy bajos de pérdidas de paquetes para la red ESPOL, ubicando menos del 1%, lo cual lo convierte en un medio seguro en pérdida de paquetes.

Ancho de Banda

La Figura 4.12 muestra el ancho de banda en el canal de reversa para la red ESPOL. Es posible observar que la cantidad de ancho de banda percibido es creciente, no obstante muy bajo en los primeros segundos del recorrido. Con un mínimo de 16.91 kbps, un máximo de 98.86 kbps y una media de 67.37 kbps, es posible evidenciar la gran variación de ancho de banda disponible para las pruebas realizadas.

Los valores de ancho de banda tan bajos que se presentan en la red tienen en parte dos explicaciones importantes: primeramente, la

posición de los puntos de acceso en conjunto con la cantidad de interferecencia presente en el medio debido a obstáculos o la presencia de otras redes influye negativamente en la capacidad de la red para brindar una óptima comunicación de voz en esa zona.

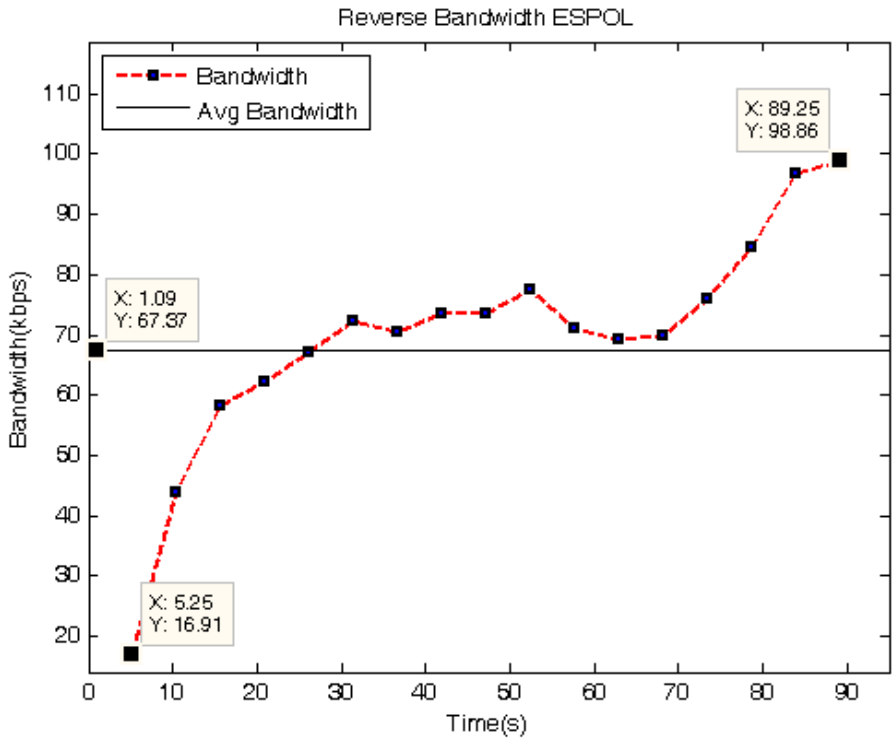

Figura 4-12– Ancho de Banda de reversa para red ESPOL.

Comparativa entre redes de Prueba.

La principal motivación de la presente tesis consiste en corroborar o descartar la superioridad de SMesh en términos de calidad de servicio a la hora de realizar llamadas de voz sobre redes inalámbricas. Es importante destacar no es posible generalizar para todos los casos

debido a la naturaleza del recorrido. No obstante, los datos sí muestran una idea del comportamiento de ambas redes para la comunicación de voz sobre IP en las instalaciones de ESPOL.

Delay

La Figura 4.13 muestra el gráfico de la comparación del Delay entre las redes SMesh y Meraki. Como se puede observar, ambas redes presentan un comportamiento similar hasta los 40 segundos aproximadamente. A partir de ese momento, ambas redes presentan una alteración en el retraso de los paquetes: por un lado, Meraki presenta un incremento de delay mientras que SMesh presenta un decremento de delay.

Esto representa un saldo positivo para SMesh en la confrontación de ambas tecnologías. Debido a que las diferencias son mínimas, se podría hablar de un empate técnico en las gráficas, no obstante, a efecto de aclarar la superioridad de una red sobre la otra en términos numéricos, la media no normalizada y del análisis no ponderado, como se puede observar en la Tabla XX, el Delay promedio para SMesh es de 19.79 milisegundos, mientras que para Meraki es de 21.2 milisegundos.

En la misma tabla se encuentra el valor de 43.74 milisegundos correspondiente a la red ESPOL.

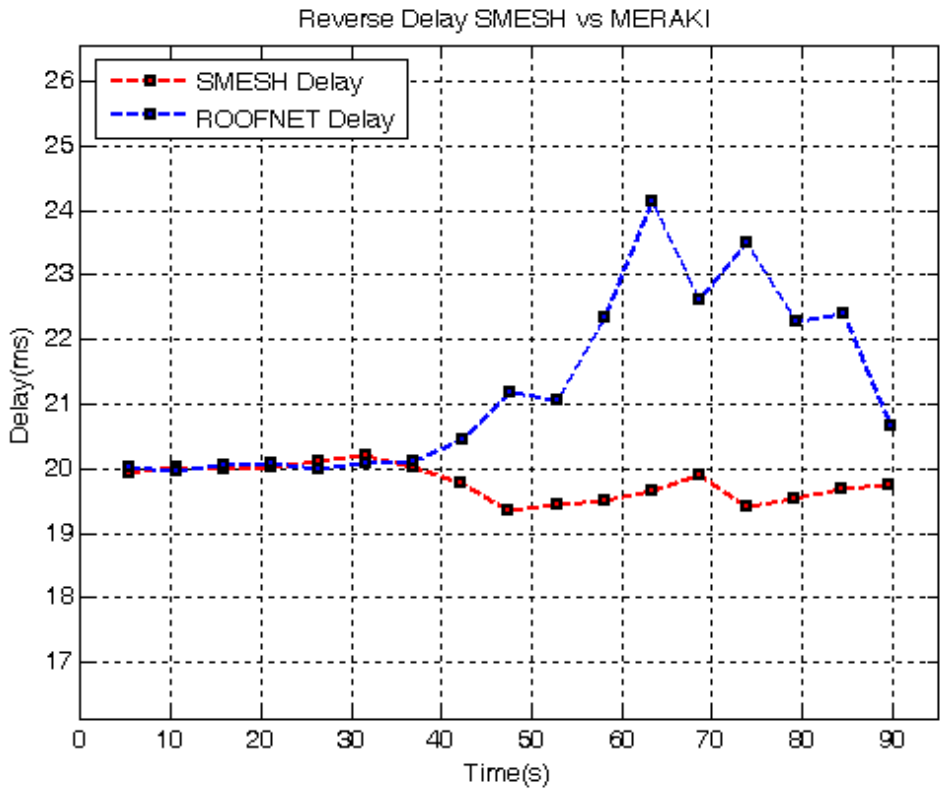

Figura 4-13 – Gráfico de Delay de reversa en red Meraki y red SMesh.

En la Figura 4.14 se muestra el gráfico de Delay de reversa para Meraki, SMesh y ESPOL. Se puede observar que las redes Wireless Mesh proveen mejores condiciones para la comunicación de voz sobre IP, debido a que presentan una naturaleza menos aleatoria.

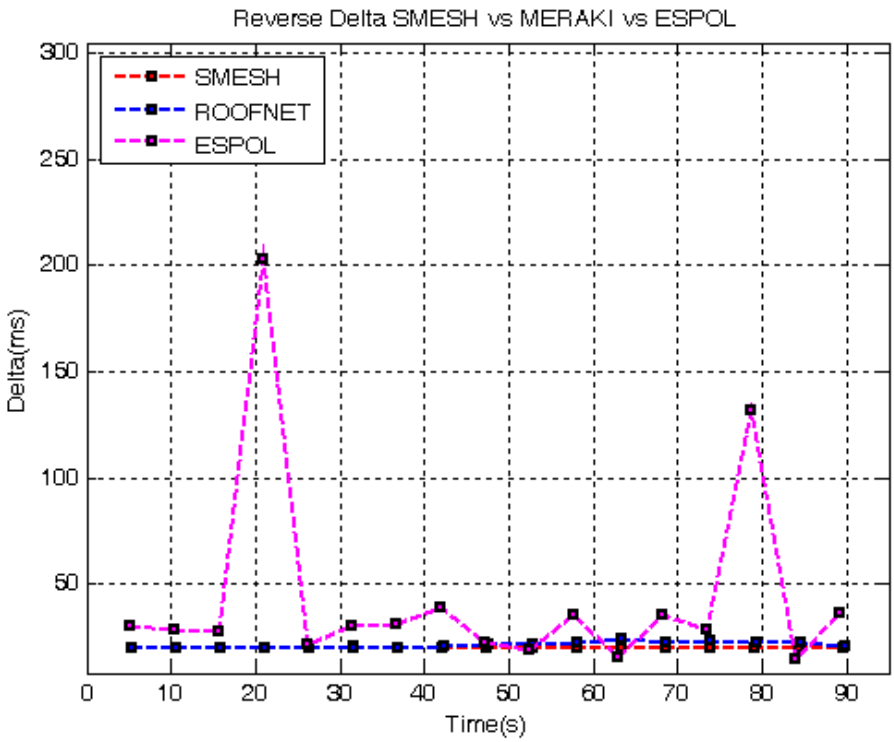

Figura 4-14 – Delta de reversa para las redes SMesh, Meraki y ESPOL.

Red	Delay Promedio (ms)
SMesh	19.79
Meraki	21.2
ESPOL	43.74

Tabla XXI - Comparativa de Delay entre redes de prueba.

La Tabla XXI ofrece una comparación en cuanto al estudio de paquetes mayores a 100 milisegundos y a su vez mayores a 150 milisegundos, así como una comparativa porcentual de aquellos paquetes que también tuvieron un atraso de más de 150 milisegundos.

Red	Delay > 100	Delay > 150	% Delay > 150
ESPOL	400	318	79.50%
Meraki	354	273	77.11%
SMesh	156	88	56.41%

Tabla XXII - Comparativa de número de paquetes con un retraso mayor a 100 milisegundos, entre redes ESPOL, Meraki y SMesh.

La tabla XXII muestra una amplia ventaja a la red SMesh frente tanto a la red Meraki como a la red ESPOL. Si bien es cierto, son valores muy pequeños y no representan un peligro para la comunicación y, de hecho, se podría declarar un empate entre las redes, no obstante, numéricamente es posible realizar una comparación, que le da una clara ventaja a SMesh.

Jitter

La Figura 4.15 muestra el gráfico comparativo de Jitter de reversa a lo largo del tiempo entre las redes Meraki y SMesh.

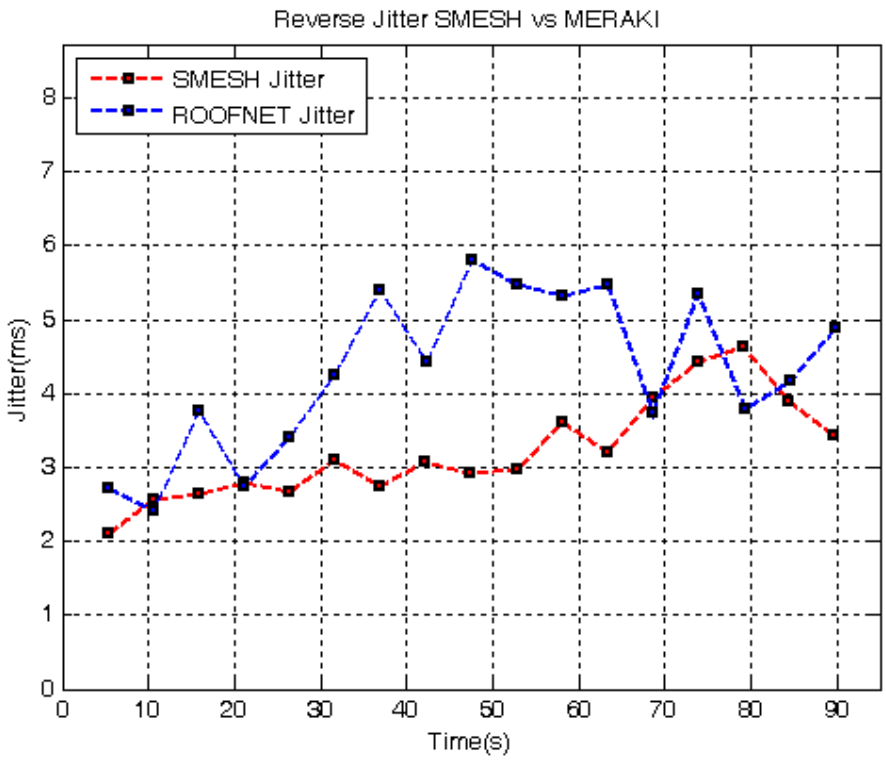

Figura 4-15 – Jitter de reversa para las redes SMesh y Meraki.

Como se puede observar, los valores de Jitter en la red SMesh son en la mayor parte de los casos inferiores a los valores de Jitter de la red Meraki.

La Figura 4.16 muestra la gráfica de Jitter para las tres redes. Esta gráfica muestra cómo la red ESPOL presenta valores mayores de Jitter en comparación a las redes Meraki y SMesh.

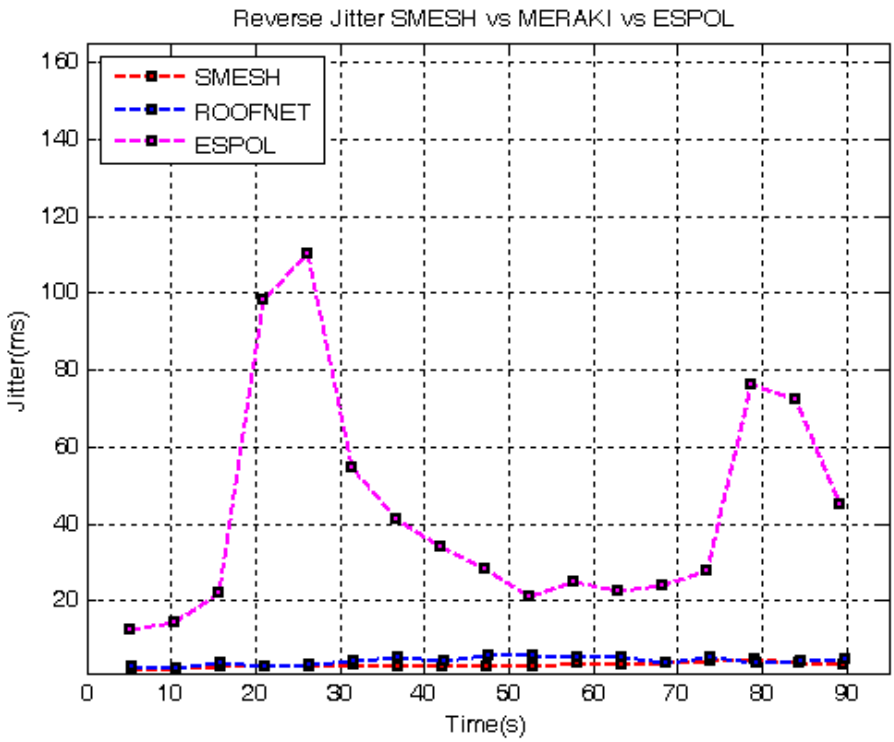

Figura 4-16 – Jitter en canal de reversa para las redes SMesh, ESPOL y Meraki.

Se podría concluir, por lo tanto, que la red SMesh presenta una mejor respuesta para el caso del Jitter, aunque ambas se encuentren dentro de los límites estimables como "óptimos" para la comunicación.

Ancho de Banda

La Figura 4.17 muestra la gráfica de ancho de banda promedio disponible para las pruebas en las redes Meraki y SMesh.

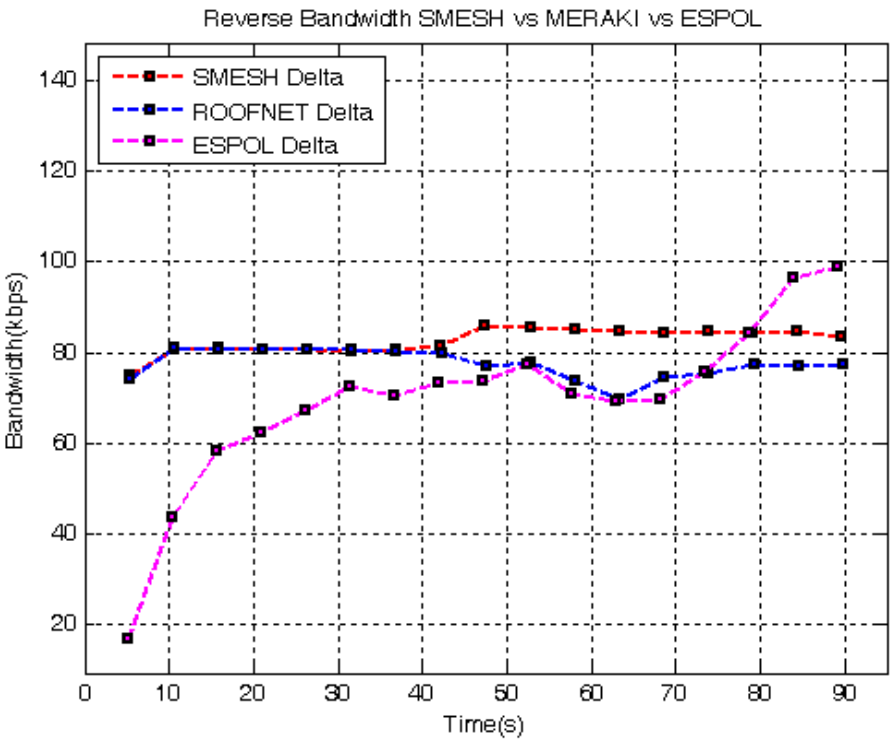

Figura 4-17– Gráfico de Ancho de Banda para las redes Meraki, ESPOL y SMesh

De acuerdo a la Figura 4.17, las variaciones en el ancho de banda percibido a lo largo del recorrido de las pruebas de voz sobre IP sobre la red ESPOL demuestra un desempeño desmejorado respecto de las redes Wireless Mesh probadas. Las gráficas de cada red muestran poco ancho de banda disponible para la comunicación.

Pruebas de Tráfico

La Tabla XXIII muestra el número máximo teórico de llamadas posibles por salto para Meraki y SMesh. Estos datos fueron obtenidos luego de

dividir el ancho de banda teórico de 54 Mbps para 80 kbps que ocupa el códec por llamada y por salto, recordando que cada salto implica un recorte del throughput a la mitad. Debido a que Meraki funciona a 54 Mbps y SMesh a 11 Mbps, el número máximo de llamadas para Meraki es muy superior al número máximo de llamadas en SMesh.

Salto	Meraki	SMesh
0	675	137
1	337	68
2	168	34

Tabla XXIII - Número máximo teórico de llamadas posibles por salto para Meraki y SMesh.

La Tabla XXIV muestra el número de llamadas recomendados por red antes de llegar al 10% de llamadas bloqueadas. El resultado es un saldo positivo para Meraki por cuanto el número de llamadas para el último salto es superior al número de llamadas para el último salto de SMesh.

Salto	Meraki	SMesh
0	85	105
1	85	55
2	50	30

Tabla XXIV - Número de llamadas recomendadas por salto para Meraki y SMesh.

No obstante, es importante destacar el aprovechamiento del ancho de banda práctico al contrastarlo con el máximo teórico. Como fue

mencionado anteriormente, el throughput máximo de la red Meraki es de 54 Mbps, con lo cual obtiene en el segundo salto un número máximo teórico de 168 llamadas mientras que, en términos prácticos el número máximo recomendado de llamadas simultáneas de 50. Esto implica que el aprovechamiento del ancho de banda, en términos prácticos resultó ser de 29.76%. Por otra parte, SMesh obtuvo un 88.23% de aprovechamiento de llamadas prácticas respecto de las teóricas, puesto que en el segundo salto el número recomendado de llamadas fue de 30 mientras que su número máximo de llamadas teóricas es de 34. Los detalles se encuentran en la Tabla XXV.

Salto	Meraki	SMesh
0	12.50%	77.00%
1	25.22%	80.88%
2	29.76%	88.23%

Tabla XXV - Rendimiento de cada red basado en ancho de banda máximo teórico y práctico.

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones son:

1. En cuanto a los resultados de los parámetros principales de calidad de servicio: la media general, así como los valores de retraso (Delay), Jitter y pérdida de paquetes en la red SMesh fueron menores que Meraki. De igual forma, la media del Ancho de Banda para la red SMesh fue superior a la media de la red Meraki. Por lo tanto, en cuanto al análisis de dichos parámetros de Calidad de Servicio, se concluye que SMesh presenta un mejor desempeño para la comunicación de voz sobre WLAN/WMN que Meraki.

2. Las redes Wireless Mesh obtuvieron un mejor desempeño que la red WLAN tradicional ESPOL en términos de Delay, Jitter y manejo de Ancho de Banda a lo largo del recorrido para las pruebas realizadas. Esto se concluye luego de identificar la superioridad en la calidad de los valores en los parámetros de las redes Wireless Mesh network en contraste con la red ESPOL. Una posible razón para dicho resultado se encuentra en el hecho de que las redes ESPOL no fueron diseñadas para el uso de voz sobre WLAN y, por tanto, los

esfuerzos se focalizaron menos en brindar una experiencia de usuario óptima para este aplicativo. Es por ello que es importante para las aplicaciones específicas (como VoWLAN) diseñar la red para soportarlas.

3. En relación a las pruebas de tráfico, la red Meraki ofreció un mayor número de llamadas concurrentes recomendadas que aseguren un bloqueo no mayor al 10% en contraste con la red SMesh. Por lo tanto, la red Meraki permite a un mayor número de usuarios utilizar la red que SMesh sin que se llegue al límite permisible óptimo de bloqueo de llamadas.

4. En cuanto al aprovechamiento del Ancho de Banda, la red SMesh presentó valores relativos mayores de utilización del throughput máximo luego de pruebas prácticas. En contraste, Meraki presentó un menor aprovechamiento del throughput máximo en términos prácticos. En el peor de los casos, el aprovechamiento del Ancho de Banda de la red SMesh es de aproximadamente cuatro veces el de la red Meraki. La conclusión de dichos resultados es que la red SMesh aprovecha mejor el Ancho de Banda para realizar llamadas de voz sobre IP.

5. En términos económicos, la implementación de una red Smesh es mucho más barata que una red Meraki: cada nodo Meraki cuesta aproximadamente 3 veces más que un nodo SMesh. La red ESPOL es mucho más cara en este sentido, puesto que el costo por router llega a ser 6 veces el de una router SMesh.

6. En términos de Calidad de Servicio subjetiva, SMesh contó con un menor número de alteraciones a lo largo de las pruebas en relación a las redes Meraki y ESPOL. Por lo tanto, en términos de experiencia de usuario, SMesh es superior a las otras redes antes mencionadas.

7. Finalmente y siguiendo la línea del planteamiento de la hipótesis propuesta por el presente trabajo, se concluye que la calidad de servicio experimentada en la red SMesh para llamadas de voz sobre IP es superior a la red Meraki en términos de parámetros de QoS, teniendo siempre como límite el número de llamadas concurrentes recomendadas mostrados en la Tabla XXIV. Esto seguirá siendo verdadero mientras el número de llamadas concurrentes no exceda el número de llamadas recomendadas por el presente trabajo para la red SMesh.

Las recomendaciones son:

1. Se recomienda tomar en consideración que el diseño de la topología de una red Wireless Mesh se diferencia del diseño de topología de una red WLAN tradicional en la cobertura de cada nodo: la cobertura de cada nodo de la red debe abarcar a cada nodo vecino inmediato. No así, en una red WLAN tradicional, las coberturas de los nodos de la red deben translaparse en un mínimo de 15%.
2. Para medir la cantidad de paquetes perdidos en redes cuya naturaleza topológica o sistemática permitan la presecia de un número muy alto de

paquetes duplicados que puedan alterar el resultado de las pruebas, se recomienda el desarrollo de software que permita medir el número de paquetes perdidos, como se explicó en el capítulo 3. El uso de un software que envíe paquetes simluando una llamada de voz sobre IP ayuda a determinar el número exacto de paquetes perdidos.

3. Se recomienda realizar estudios de QoS para VoWLAN en áreas de interés dentro de la ESPOL y continuar con la idea de crear una red VoWLAN para el personal administrativo y docente. Se recomienda asimismo tomar en consideración y guía el presente trabajo, así como el software que organiza y muestra en gráficos los paquetes y el encargado de medir el número de paquetes perdidos.

4. Es altamente recomendable realizar un estudio del número de posibles usuarios que tenga la red y de la posible concentración de tráfico. Dependiendo de aquellos datos, podría variar el número de puntos de acceso disponibles y número de saltos por zona.

ANEXOS

Script de Python para enviar paquetes:

```
import socket
import time

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
contador=0
while True:
    a="0"
    k=140-repr(contador).__sizeof__()
    for i in range(0,k):
        a=a+"0"
    data=repr(contador)+"-"+a
    sock.sendto(data,('200.126.12.109',8477))
    time.sleep(0.02)
    print "paquete enviado..."
    contador=contador+1
    if contador==5000:
        break
sock.close();
```

Script de Java para recibir paquetes (dependencias: JPcap 0.7):

```
t1 = new Date().getTime();
NetworkInterface[]
lists=jpcap.JpcapCaptor.getDeviceList();
System.out.println("\n\t\t***jSniffer - Sniffer creado en
Java por Juan Carlos Basurto***\n");
int numero=0;
JpcapCaptor
jpcap=JpcapCaptor.openDevice(JpcapCaptor.getDeviceList()[
numero],1000,false,20);
jpcap.setFilter("port 8477", true);
System.out.println("Conexión exitosa!.");
System.out.println("MAC address:");
for (byte b :
JpcapCaptor.getDeviceList()[numero].mac_address)
System.out.print(Integer.toHexString(b&0xff) + ":");
new Inner("").start();
jpcap.loopPacket(-1,new JSniffer());
```

//métodos para analizar los resultados luego de un tiempo t

BIBLIOGRAFIA

1. Instituto de Ingenieros Eléctricos y Electrónicos, Estándar IEEE-802.11, http://standards.ieee.org, 2004.
2. Jim Geier. Deploying Voice over Wireless LAN. Cisco Press, 2007.
3. David D. Coleman, David A. Westcott. Certified Wireless Network Administrator Study Guide. Wiley Publishing, 2006.
4. Yan Zhang, Jijun Luo, Hongling Hu. Wireless Mesh Networking: Architectures, Protocols and Standards. Auerbach Publications, 2007.
5. Python para Todos, Raúl González Duque, Creative Commons, 2007.
6. Niculescu D., Ganguly S., Kim K., Navda V., Kashyap A. Performance Optimizations for Deploying VoIP Services in Mesh networks, 2006.
7. Amir Y., Danilov C., Musaloi-Elefteri R., Rivera N. The SMesh Wireless Mesh Network, 2009.
8. Amir Y., Danilov C., Musaloi-Elefteri R., Rivera N. Fast Handoffs for Seamless Wireless Mesh Networks, 2006.
9. Niculescu D., Ganguly S., Kim K., Izmailov R., Performance of VoIP in a 802.11 Wireless Mesh Network, 2006.

10. Chen Y., Smavatkul N., Emeott S. Power Management for VoIP over IEEE 802.11 WLAN.
11. MIT Roofnet Project Website http://pdos.csail.mit.edu/roofnet/design/.
12. Elliote Rusty Harold. Java Networking Programming: 3rd Edition. O'Reilly Media, 2005.
13. Norman Matloff, Tutorial on Networking programming with Python, http://heather.cs.ucdavis.edu/~matloff/Python/PyNet.pdf, 2009.
14. HP-SipP Traffic Generator Manual in PDF http://sipp.sourceforge.net/doc/reference.pdf, 2004.
15. Keita Fujii, JPcap 0.7 Tutorial http://netresearch.ics.uci.edu/kfujii/jpcap/doc/tutorial/index.html, 2007.
16. Jarmo Prokkola, Mikko Hanski, QoS Measurement Methods and Tools http://ew.thales.no/common/VTT/T.4.1.%20QoS%20Measurement%20Methods%20and%20Tools.pdf, 2005.
17. Yin Chen, Handoff on WLAN Mesh Networks, http://www.cnri.dit.ie/research.mesh.yin.html, Communications Network Research institute, 2008.
18. Denis Bakin, Evolution of 802.11 (Physical Layer), https://www.okob.net/texts/mydocuments/80211physlayer/, 2007.
19. The Real-Time Transport Protocol http://www.networksorcery.com/enp/protocol/rtp.htm, 1998.