CAPITULO I
INTRODUCCION

CAPITULO I

Introducción

I.1. Hipótesis

Con la implementación de una red inalámbrica *Mesh* en el campus universitario de la UPDS, se provee conectividad constante a la red e Internet a todos sus estudiantes y docentes, teniendo una cobertura extendida desde los bloques A y B, hasta la Academia Local Cisco UPDS y a las áreas de recreación.

I.2. Justificación

Las TIC (Tecnologías de Información y comunicación) ofrecen nuevas oportunidades y facilidades de enseñanza y aprendizaje y su incorporación a las universidades constituyen un objetivo estratégico para fomentar la educación superior. Se ha observado que el campus de la "Universidad Privada Domingo Savio" no cuenta con una cobertura extensa y no proporciona conectividad constante a la red e Internet, dificultando las actividades académicas de estudiantes y docentes. Por tal motivo se utilizará la estrategia "Incorporación de TIC en la educación universitaria", la cual consiste en el diseño de una red inalámbrica *Mesh.* Se hará a conocer a todo el sector estudiantil y plantel docente, de los múltiples beneficios que traerá la creación de una nueva red de datos para el intercambio de información.

I.2.1. Justificación Tecnológica

Estamos viviendo un tiempo de cambios acelerados de la tecnología, por lo que es importante que una Universidad esté actualizada y cuente con tecnología de punta para poder brindar una mejor calidad de enseñanza y así formar profesionales competentes.

I.2.2. Justificación Académica

Se efectuaron las investigaciones necesarias para el desarrollo del proyecto, además de aplicar y poner en práctica todos los conocimientos que hemos adquiridos durante los años de estudio en la universidad. Habiendo escogido como especialización el área de redes, podemos diseñar una solución tecnológica que permita satisfacer las necesidades

de comunicación de una institución tan importante como la UPDS en particular.

I.2.3. Justificación Social

La UPDS Tarija es una universidad privada que abrió sus puertas hace 6 años con la finalidad de brindar excelencia en educación y ofrecer una mejor enseñanza a sus estudiantes. Para poder competir con las demás universidades de la región, tiene la necesidad de estar al día con los avances tecnológicos que puedan facilitar las actividades académicas de estudiantes y/o docentes.

I.3. Delimitación

I.3.1 Límite Sustantivo

El proyecto se enfocará en el diseño de una red inalámbrica *Mesh* con una cobertura total del campus universitario de la UPDS. También el diseño contemplará teóricamente el uso de VLANs para una mejor distribución de la información, estando separados voz, video y datos en VLANs diferentes. No se podrá llevará a cabo una simulación del diseño para demostrar su funcionalidad y capacidad de conectividad, debido a la falta de un simulador existente para esta red especifica.

I.3.2 Límite Temporal

Tomando en cuenta el reciente avance de la tecnología *Mesh* y que aún no se ha establecido un estándar final y un protocolo específico para su creación, se prevé que la red inalámbrica *Mesh* a ser diseñada tendrá una vida útil de 5 años.

I.3.3 Límite Geográfico

El diseño de la red inalámbrica, tendrá una cobertura total de conexión dentro del área geográfica del campus universitario de la UPDS, es decir los bloques: A, B, las áreas de recreación y la Academia Local Cisco UPDS.

I.4. Planteamiento del problema

Debido a la reciente creación del campus universitario de la UPDS la implementación de nuevas tecnologías es aun escasa, de esta manera se puede evidenciar que el servicio actual es muy limitado, ineficiente y no cumple con los requerimientos del usuario. Los demás predios de la universidad como ser: la academia Cisco y las áreas de recreación no cuentan con ningún tipo de conexión WiFi que permita acceder a la red e Internet.

I.4.1. Árbol de Problemas

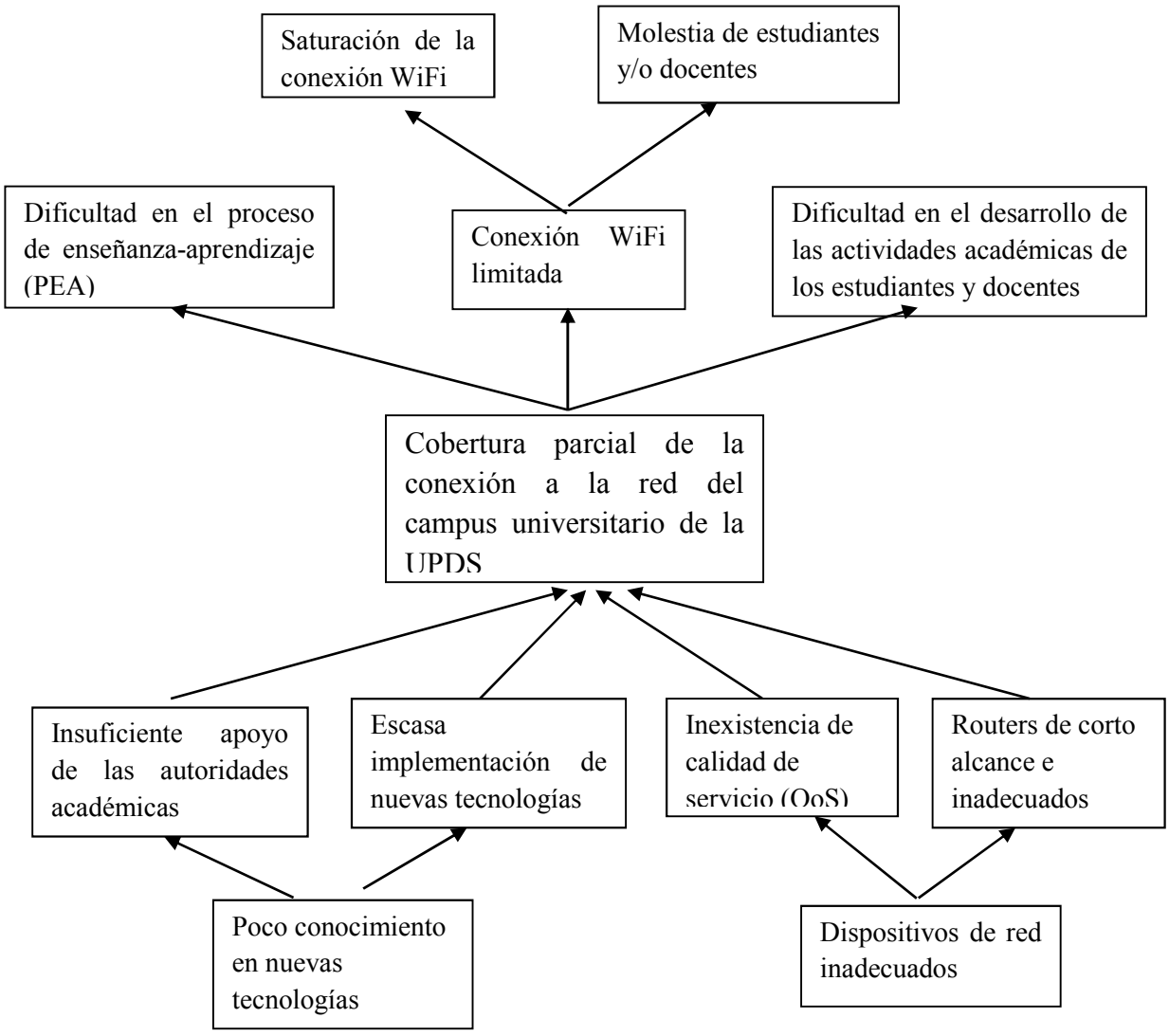

Figura I.1 Árbol de Problemas

I.4.2. Árbol de Objetivos

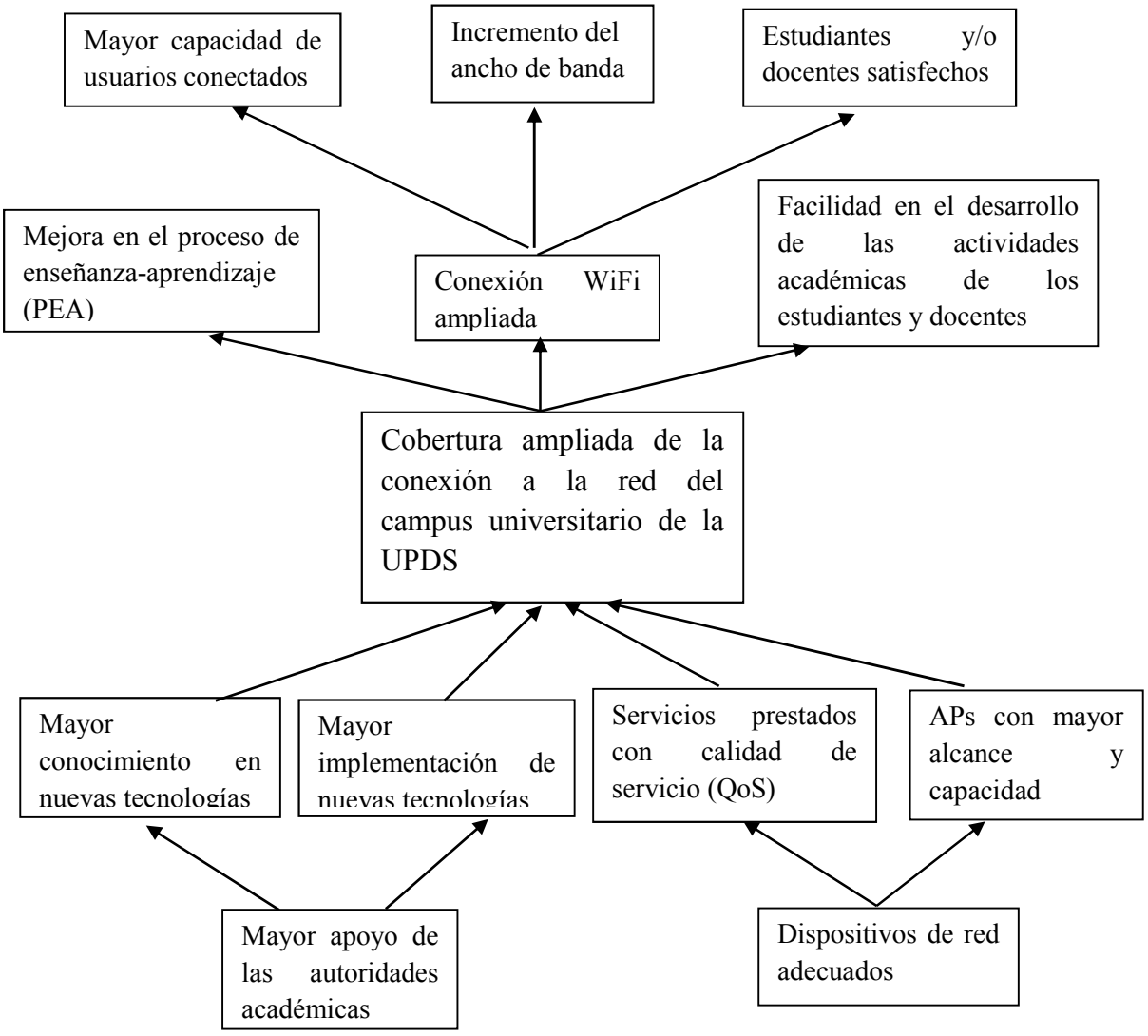

Figura I.2 Árbol de Objetivos

I.5. Objetivo General

El presente proyecto tiene como objetivo principal: "Ampliar la cobertura de la red para proporcionar conectividad constante, con la finalidad de brindar un acceso fácil y rápido a la red e Internet del campus universitario de la Universidad Privada Domingo Savio".

I.6. Metodología

I.6.1. Tipo de Investigación o Estudio

Se realizará una investigación de tipo documental, ya que se recopilará y seleccionará información de diferentes fuentes acerca de todo lo que se refiera a la tecnología WiFi y redes inalámbricas *Mesh*, para así obtener el conocimiento necesario que nos permita diseñar un proyecto factible tecnológica y económicamente.

I.6.2. Fuentes de Información

Fuentes de Información primarias

- Entrevistas con el administrador del Departamento de Sistemas de la UPDS
- Observación

Fuentes de Información secundarias

- Información encontrada en páginas web
- Libros
- Proyectos similares

I.6.3. Métodos

Para el presente proyecto se utilizará el método deductivo, ya que se realizará un estudio global de una red inalámbrica *Mesh*, para después aplicar sus características investigadas en el diseño de este tipo de red, cumpliendo de esta manera los requerimientos que presenta la UPDS.

I.6.4. Procedimientos

Recopilación de Información

Primero se recopilará información acerca del estado actual de la red WiFi de la UPDS y de la forma en que se administran los usuarios conectados y después se realizará una extensa revisión bibliográfica con la finalidad de adquirir conocimientos sobre las redes inalámbricas *Mesh* y VLANs, para llevar a cabo un buen estudio de investigación.

Diseño de la red inalámbrica Mesh

Luego de tener una base teórica bien fundamentada acerca de la tecnología *Mesh* y VLANs, se procederá al diseño de la red con soporte inicial de tráfico de datos y dejando el tráfico de voz y video a futuro crecimiento de la red, de manera que satisfaga las necesidades de conectividad de la UPDS. Para esto se tomará en cuenta las características de dicha institución como ser: la cantidad de frecuencia de usuarios y la extensión territorial o área geográfica.

Determinación de Presupuesto

Luego de terminar el proceso de diseño, se determinará los costos de *hardware* que son necesarios para la implementación de la red diseñada.

CAPITULO II
MARCO TEORICO

CAPITULO II

Marco Teórico

II.1. Red de Datos [1]

Se denomina red de datos a aquellas infraestructuras o redes de comunicación, que se han diseñado específicamente, para la transmisión de información mediante el intercambio de datos.

Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la conmutación de paquetes y se clasifican de acuerdo ha: su tamaño, la distancia que cubre y su arquitectura física.

II.2. Red de Computadoras [2]

II.2.1. Definición

La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresoras. Una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo. Para compartir impresora basta con un switch, pero si se desea compartir eficientemente archivos y ejecutar aplicaciones de red, hace falta una tarjeta de interfaz de red (NIC NetWare interface Cards) y cables para conectar los sistemas. El objetivo fundamental de conectar ordenadores es el de poder compartir recursos. Así pues podemos disponer de una red local de varios ordenadores.

Una red es el conjunto de dispositivos físicos "*hardware*" y de programas "*software",* mediante el cual podemos comunicar ordenadores para compartir recursos (impresoras, CD-ROM) así como trabajo (tiempo de cálculo, procesamiento de datos). A cada uno de los ordenadores conectados a la red se les denomina "nodo". Se considera que una red es local si solo alcanza unos pocos kilómetros.

II.2.2. Tipos de Redes [3]

II.2.2.1. Red de Área Local (LAN)

Las redes de área local, suelen ser una red limitada, ejem.: la conexión de equipos dentro de un único edificio, oficina o campus. La mayoría son de propiedad privada.

II.2.2.2. Red de Área Metropolitana (MAN)

Las redes de área metropolitanas, están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LANs, resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusiva de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas.

II.2.2.3. Red de Área Extensa (WAN)

Las redes de área extensa, son aquellas que proporcionan un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y/o redes privadas, que pueden extenderse alrededor del globo.

II.3. Ancho de Banda [4], [5]

El ancho de banda es un concepto sumamente importante para los sistemas de comunicación. Dos formas de considerar el ancho de banda, que resultan importantes en el estudio de las redes, son: el ancho de banda analógico y el ancho de banda digital. En computación de redes y en ciencias de la computación, ancho de banda digital, ancho de banda de red o simplemente ancho de banda, es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él (kbit/s, Mbit/s, entre otros).

Ancho de banda digital puede referirse también, como *bit de ratio medio*, definida como la cantidad total de datos dividida por el tiempo del sistema de lectura. Algunos autores prefieren menos términos ambiguos tales como: *grueso de índice bits*, *índice binario de*

la red, *capacidad de canal* y rendimiento de procesamiento, para evitar la confusión entre el ancho de banda digital en bits por segundo y el ancho de banda análogo en hertzios.

II.3.1. Velocidades de Transferencia

Esta es una tabla que muestra los máximos anchos de banda, de diferentes tipos de conexiones a Internet:

56 kbit/s	Modem / Marcado telefónico
1.544 Mbit/s	T1
10 Mbit/s	Ethernet
11 Mbit/s	Inalámbrico 802.11b
43.232 Mbit/s	T3
54 Mbit/s	Inalámbrico-G 802.11g
100 Mbit/s	Ethernet Rápida
155 Mbit/s	OC3
300 Mbit/s	Inalámbrico-N 802.11n
622 Mbit/s	OC12
1000 Mbit/s	Ethernet Gigabit
2.5 Gbit/s	OC48
9.6 Gbit/s	OC192
10 Gbit/s	Ethernet de 10 Gigabit

Tabla II.1 Velocidades de Transferencia

II.4. **Conectividad** [6], [7], [8], [9]

La conectividad es un concepto que, describe la capacidad de dos o más elementos hardware o software, para trabajar conjuntamente y transmitir datos e información en un entorno informático heterogéneo. Dos importantes aspectos de la conectividad son:

a. Las redes de cómputo: las computadoras pueden enlazarse con otros tipos de computadoras de diferente capacidad, como: micro, mini, o macrocomputadoras, formando redes de cómputo. Una de las finalidades de esta interconexión, además de la comunicación por sí misma, es la de compartir datos y recursos.

b. Superautopista de la información: La tecnología de Internet es el cimiento de la llamada superautopista de la información, una red teórica de computadoras y comunicaciones informáticas que en el futuro proporcione a colegios, bibliotecas, empresas y hogares, acceso universal a una información de calidad que: eduque, informe y entretenga.

II.4.1. Requerimientos para la conectividad entre los dispositivos

Un medio de transmisión y dos o más dispositivos que manejen los mismos protocolos de trasferencia (TCP/IP, NetBEUI, IPX/SPX, DecNet, AppleTalk). Al conjunto de estos dos elemento mencionados y agregando que estos interactúan, se llama *conectividad* y se dice que los dispositivos están en red. Cuantas más conexiones (nodos o computadoras) se agregan, estos forman una red cada vez mayor y reciben nombre diferentes.

II.5. **Modelo OSI** [10], [11], [12], [13]

El **modelo de interconexión de sistemas abiertos**, también llamado **OSI** (en inglés *Open System Interconnection*) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización (ISO) en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Proporciona a los fabricantes, estándares que aseguran mayor

compatibilidad e interoperabilidad entre distintas tecnologías de red producidas mundialmente.

II.5.1. Modelo de referencia OSI

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles, donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara, en donde puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza, como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.

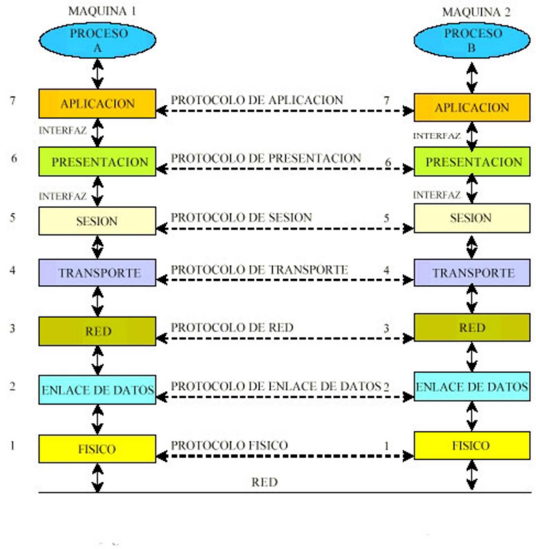

Figura II.1 Modelo OSI

El modelo especifica el protocolo que debe ser usado en cada capa y suele hablarse de modelo de referencia, ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas.

II.5.2. Estructura del Modelo OSI

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

a) **Estructura multinivel:** Se diseñó una estructura multinivel, con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas. El nivel superior utiliza los servicios de los niveles inferiores. Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

b) **Puntos de acceso**: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

c) **Dependencias de Niveles**: Cada nivel es dependiente del nivel inferior y también del superior.

d) **Encabezados**: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora, se entere de que su similar en la computadora emisora está enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje está constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria, aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como *la computadora destino* retira los encabezados en orden inverso a como fueron incorporados en la *computadora origen,* finalmente el usuario sólo recibe el mensaje original.

e) **Unidades de información:** En cada nivel, la unidad de información tiene diferente nombre y estructura.

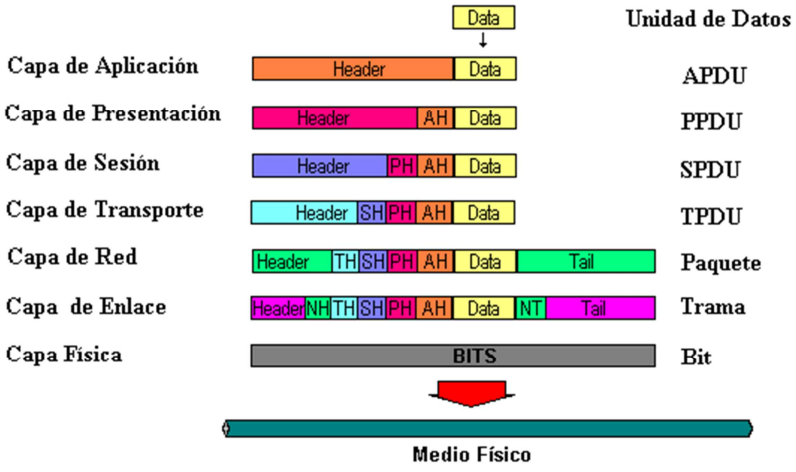

Figura II.2 Estructura del Modelo OSI

II.5.3. Capas del modelo OSI

II.5.3.1. Capa Física

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico, como a la forma en la que se transmite la información. En la capa física, las tramas procedentes de la capa de enlace de datos, se convierten en una secuencia única de bits que puede transmitirse por el entorno físico de la red. Los protocolos de la capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento, para activar y desactivar conexiones físicas para la transmisión de bits hacia y desde un dispositivo de red.

II.5.3.2. Capa de Enlace de datos

La función principal de la capa de enlace de datos, es lograr una comunicación eficiente y confiable entre dos extremos de un canal de transmisión. Para ello, la capa de enlace de datos realiza las siguientes funciones:

- Armado y separación de tramas
- Detección de errores
- Control de flujo

- Adecuación para el acceso al medio
- Subcapa LLC
- Subcapa MAC

II.5.3.3. Capa de Red

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes y se pueden clasificar en: protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)
- Enrutamiento: permiten seleccionar las rutas (RIP,IGRP,EIGP,OSPF,BGP)

El objetivo de la capa de red, es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan *routers*. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne.

II.5.3.4. Capa de Transporte

La capa de transporte, es la encargada de controlar el flujo de datos entre los nodos que establecen una comunicación; los datos no solo deben entregarse sin errores, sino además en la secuencia esperada. La capa de transporte se ocupa también de evaluar el tamaño de los paquetes, con el fin de que estos tengan el tamaño requerido por las capas inferiores del conjunto de protocolos. El tamaño de los paquetes lo dicta la arquitectura de red que se utilice.

La capa de transporte define los servicios para: segmentar, transferir y reensamblar los datos, para las comunicaciones individuales entre dispositivos finales. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP.

De la misma manera que hay dos tipos de servicios de red, hay dos tipos de servicios de transporte, orientados y no orientados a la conexión, como ser:

- **TCP (Transmission Control Protocol):** es un protocolo orientado a la conexión, que proporciona flujos de información seguros y confiables.
- **UDP (User Datagram Protocol):** es un protocolo no orientado a la conexión, muy sencillo (básicamente el paquete IP más un encabezado) y no seguro.

II.5.3.5. Capa de Sesión

Esta capa es la que se encarga de mantener y controlar, el enlace establecido entre dos computadoras que están transmitiendo datos de cualquier tipo. Una vez establecida la sesión entre los nodos participantes, la capa de sesión pasa a encargarse de ubicar puntos de control en la secuencia de datos. De esta forma, se proporciona cierta tolerancia a fallos dentro de la sesión de comunicación.

Si una sesión falla y se pierde la comunicación entre los nodos, cuando después se restablezca la sesión, solo tendrán que volver a enviarse los datos situados detrás del último punto de control recibido. Así se evita el tener que enviar de nuevo todos los paquetes que incluía la sesión.

II.5.3.6. Capa de Presentación

La capa de presentación puede considerarse el traductor del modelo OSI. Esta capa toma los paquetes de la capa de aplicación y los convierte a un formato genérico que puedan leer todas las computadoras. Por ejemplo: los datos escritos en caracteres ASCII se traducirán a un formato más básico y genérico. El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, los datos lleguen de manera reconocible.

En esta capa se tratan aspectos tales como: la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. La capa de presentación también se encarga de cifrar los datos, así como de comprimirlos para reducir su tamaño.

II.5.3.7. Capa de Aplicación

La capa de aplicación proporciona los medios para la conectividad de extremo a extremo, entre individuos de la red humana que usan red de datos. Esta capa suministra las herramientas que el usuario de hecho ve, también ofrece los servicios de red relacionados con estas aplicaciones de usuario, como: correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Por UDP pueden viajar DNS y RIP.

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones, el número de protocolos crece sin parar.
Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente.

II.6. Internet en la educación [14], [15]

II.6.1. Concepto

Internet es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que las componen, funcionen como una red lógica única de alcance mundial. Uno de los servicios que más éxito ha tenido en Internet, ha sido la World Wide Web (WWW o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos.

La WWW es un conjunto de protocolos, que permite de forma sencilla, la consulta remota de archivos de hipertexto. Existen, por lo tanto, muchos otros servicios y protocolos, aparte de la Web, en Internet: el envío de correo electrónico (SMTP), la

transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencial, la transmisión de contenido y comunicación multimedia, telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

II.6.2. Internet y sociedad

Internet tiene un impacto profundo en: el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web, ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales, animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos. En este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

II.6.3. Internet y su evolución

Inicialmente el Internet tenía un objetivo claro. Se navegaba en Internet para algo muy concreto, como búsquedas de información generalmente. Ahora quizás también, pero sin duda alguna, hoy es más probable perderse en la red, debido al inmenso abanico de posibilidades que brinda. Hoy en día, la sensación que produce Internet es: un ruido, una serie de interferencias, una explosión de ideas distintas; de: personas diferentes, de pensamientos distintos de tantas posibilidades que, en ocasiones puede resultar excesiva.

El crecimiento o más bien la incorporación de tantas personas a la red, hace que las calles, de lo que en principio era una pequeña ciudad llamada Internet, se conviertan en todo un planeta, extremadamente conectado entre sí y entre todos sus miembros. El hecho de que Internet haya aumentado tanto, implica una mayor cantidad de relaciones virtuales entre personas.

II.6.4. Internet en la educación superior

La educación no ha escapado a la influencia de Internet. Son pocas las universidades que disponen y ofertan: cursos, programas o materiales de estudio, basados en la red tanto para la docencia convencional, como para la educación a distancia. Algunas universidades están poniendo en práctica un modelo mixto, que combina la oferta presencial de enseñanza superior, con un espacio virtual que permita al alumno cursar estudios a distancia. Aunado a esto, varias universidades empiezan a publicar tutoriales o materiales didácticos para el WWW, elaborados por profesores para los alumnos de sus asignaturas. Pero en la mayor parte de los casos, esta práctica se realiza individual y solitariamente, gracias al esfuerzo e interés personal.

El Internet también ha cambiado los métodos de investigación y de recolección de datos. Actualmente la mayoría de los estudiantes y profesores buscan información en Internet antes que en una biblioteca. Entre muchas de las ventajas de utilizar la *red de redes* para estos fines están: la rapidez con que se puede encontrar la información; la gran cantidad de datos que se pueden conseguir acerca de un mismo tema de interés; el bajo costo que significa el no tener que comprar determinado libro; etc.

II.6.5. El Internet en la pedagogía

A continuación se enlistan algunos de los cambios pedagógicos más sustantivos que provocan la utilización de las redes informáticas en el ámbito de la educación superior:

a. Las redes informáticas permiten extender los estudios universitarios a quienes por distintos motivos no pueden acceder a las aulas.

Este es uno de los efectos más llamativos e interesantes de las redes informáticas al servicio de la educación, se rompen las barreras del tiempo y el espacio para desarrollar las actividades de enseñanza y aprendizaje. Con el Internet es posible que las instituciones universitarias, realicen ofertas de cursos y programas de estudio virtuales, de modo que distintas personas, que por motivos de edad, profesión o de lejanía no pueden acudir a las aulas convencionales, cursen estos estudios desde su hogar.

b. La red rompe con el monopolio del profesor como fuente principal del conocimiento.

Hasta la fecha, el docente era la única referencia que tenía el alumnado para el acceso al saber. El profesor posee el monopolio del conocimiento especializado de la asignatura, domina: los conceptos, las teorías, los procedimientos, los métodos, la bibliografía, las escuelas o tendencias. Para cualquier alumno, la única forma alternativa de acceso al conocimiento de una disciplina científica, era la búsqueda de textos en una biblioteca, lo cual representaba una tarea tediosa, larga y limitada.

Hoy en día, Internet, permite romper ese monopolio del saber. Cualquier alumno puede acceder al website, no sólo de su profesor, sino al de profesores de otras universidades de su país y por extensión del resto del mundo. De este modo, un alumno puede acceder a una enorme variedad de propuestas docentes de una misma disciplina. Con Internet tiene a su alcance: la bibliografía, el temario o la documentación de muchos centros universitarios.

c. Con Internet, el proceso enseñanza-aprendizaje se convierte en una permanente búsqueda, análisis y reelaboración de informaciones obtenidas en las redes.

Desde un punto de vista psicodidáctico, una de las innovaciones más profundas que provoca la incorporación de las redes informáticas a la metodología de enseñanza universitaria, es que el modelo tradicional de transmisión y recepción de la información,

a través de lecciones expositivas, deja de tener sentido y utilidad. Todo el conocimiento o saber que un docente necesita comunicar a su alumnado, puede ser "colgado" en la red de modo que lo tengan disponible cuando lo deseen.

Pero lo más relevante, es que puede utilizarse **Internet** como una gigantesca biblioteca universal, en la que el aula universitaria o el hogar, se convierten en puntos de acceso abiertos, a todo el entramado mundial de computadoras interconectadas en el World Wide Web.

d. La utilización de redes informáticas en la educación requieren un aumento de la autonomía del alumnado.

Esta idea vinculada estrechamente con la anterior, indica que las tecnologías de la información y comunicación, en el contexto de la educación superior, exigen un modelo educativo caracterizado, entre otros rasgos, por el incremento de la capacidad decisional del alumnado sobre su proceso de aprendizaje, así como por una mayor capacidad para seleccionar y organizar su curriculum formativo. Es una idea valiosa desde un punto de vista pedagógico y que tiene que ver con el concepto de aprendizaje abierto y flexible, entendido éste, como la capacidad que se le ofrece al alumno para que establezca su propio ritmo e intensidad de aprendizaje, adecuándolo a sus intereses y necesidades.

e. El horario y el espacio de las clases deben ser más flexibles y adaptables a una variabilidad de situaciones de enseñanza.

La incorporación de las nuevas tecnologías de la comunicación supone una ruptura en los modos y métodos tradicionales de enseñanza, en consecuencia, sus efectos también tienen que ver con nuevas modalidades de enseñanza. El horario y distribución del espacio para la actividad docente, han sido útiles para un método de enseñanza basado en la transmisión oral de la información por parte del docente, a un grupo más o menos amplio de alumnos. Sin embargo, un modelo educativo que se basa en la utilización de los recursos telemáticos, significará que el tiempo y el espacio adoptarán un carácter flexible. Lo relevante desde un punto de vista pedagógico, en consecuencia, no es el

número de horas que están juntos en la misma clase, el docente y el alumno, sino al cumplimiento por parte de los alumnos de las tareas establecidas por el docente. Uno de los efectos más interesantes de las nuevas tecnologías sobre la enseñanza, es que ésta adoptará un carácter de semi-presencialidad, es decir, el tiempo de aprendizaje debe ser repartido equitativamente, entre la realización de tareas con máquinas y entre la participación en grupos sociales, para: planificar, discutir, analizar y evaluar las tareas realizadas.

f. Las redes transforman sustantivamente los modos, formas y tiempos de interacción entre docentes y alumnos.

Las nuevas tecnologías permiten incrementar considerablemente, la cantidad de comunicación entre el profesor y sus alumnos, independientemente del tiempo y el espacio. En la enseñanza convencional, la comunicación se produce cara a cara en horarios establecidos al efecto. Con las redes informáticas es posible que esta interacción se produzca, mediante la videoconferencia o a través del *chat* o bien mediante el correo electrónico o el foro de discusión.

Esto significa que cualquier alumno puede: plantear una duda, enviar un trabajo, realizar una consulta, desde cualquier lugar y en cualquier momento. Lo cual implicará una reformulación del papel docente del profesor. El modelo de enseñanza a través de redes, hace primar más el rol del profesor como un "tutor" del trabajo académico del alumno, que un expositor de contenidos.

g. El Internet permite y favorece la colaboración entre docentes y estudiantes más allá de los límites físicos y académicos de la universidad a la que pertenecen.

Los sistemas de comunicación e intercambio de información que son posibles mediante el WWW, chat, e-mail, ftp, videoconferencia, foros, etc. facilitan que grupos de alumnos y/o profesores, constituyan comunidades virtuales de colaboración en determinados temas o campos de estudio. De esta forma, cualquier docente puede ponerse en contacto

con colegas de otras universidades y compartir experiencias educativas de colaboración entre sus alumnos.

II.6.6. Niveles de integración y uso de las redes informáticas en la enseñanza universitaria

El Internet, representa un factor o catalizador radical para la renovación y mejora pedagógica de la enseñanza universitaria. Sin embargo, el uso de Intern**et** con fines docentes, no es un proceso fácil de poner en práctica y no siempre se logra realizar satisfactoriamente. Todo proceso de renovación educativa, es un proceso complejo sometido a la variabilidad de numerosos factores. Las redes informáticas, por su propia naturaleza, posibilitan que existan distintos niveles de uso y desarrollo de acciones educativas en torno a las mismas. En la docencia universitaria las formas de uso e integración de **Internet,** pueden oscilar entre la elaboración de pequeñas experiencias docentes, como publicar una página web con el programa de la asignatura, hasta la creación y puesta en marcha de todo un sistema de formación a distancia *on line,* desarrollado institucionalmente por una universidad.

II.6.7. Internet como fuente de investigación

Actualmente el acceso a Internet, es cada vez más frecuente por parte de los estudiantes al momento de buscar información. El uso de Internet como herramienta de investigación, se ha convertido en poco tiempo en una gran alternativa al uso de las bibliotecas. Es común encontrar dentro de una biblioteca una sala de cómputo con acceso a Internet.

Se hace evidente pues, la interrelación que existe entre estas dos grandes fuentes de información. Sin embargo, es notorio el hecho de que cada vez más, el estudiante prefiere obtener los datos que necesita para su investigación, a través de la "autopista de la información" y no de la biblioteca tradicional. Entre las principales ventajas que ofrece el uso de Internet como fuente de información tenemos:

- El acceso a una cantidad mayor de fuentes de información, con motores de búsqueda especializados que ahorran el tiempo de búsqueda de los datos.
- El acceso a herramientas informáticas para el intercambio de la información, tales como: e-mail, charlas en línea (chats), forum de discusión, etc.
- El ahorro de tiempo permite culminar con más rapidez los trabajos de investigación.
- El acceso a grandes bases de datos, ofreciendo la oportunidad de realizar un trabajo de mayor calidad.
- El acceso directo a la tecnología moderna, que obliga al usuario a mantenerse al día en los cambios tecnológicos. Esto incide positivamente en el desarrollo cultural del individuo.
- Sirve como complemento del aprendizaje a la par del uso de las bibliotecas tradicionales.

Quizá la posible gran desventaja que podríamos encontrar en un uso muy frecuente de Internet, para buscar información, es que ciertos estudiantes se dedican a copiar textualmente monografías que se encuentran en la red, sin hacer uso de su creatividad y de su capacidad de análisis. Esto evidentemente afecta negativamente el desarrollo intelectual de estos estudiantes.

II.7. Red inalámbrica [16], [17]

II.7.1. Definición

El término **red inalámbrica** *(Wireless network,* en inglés), es un término que se utiliza en informática, para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos. Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema. Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías que se diferencian

por: la frecuencia de transmisión que utilizan y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas, permiten que los dispositivos remotos se conecten sin dificultad, ya sea que se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente, como pasa con las redes cableadas. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

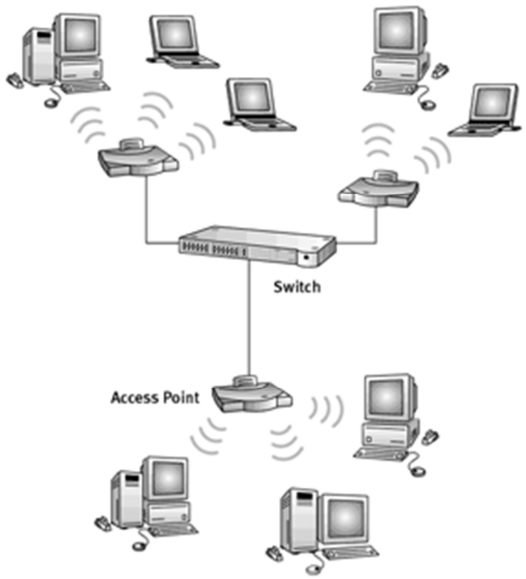

Figura II.3 Red Inalámbrica

Por otro lado, existen algunas cuestiones relacionadas con la regulación legal del *espectro electromagnético*. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Una de sus principales ventajas y muy notable, son los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos. Pero también tiene una desventaja

considerable, ya que para este tipo de red, se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos. En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras.

II.7.2. Categorías

Existen dos categorías de las redes inalámbricas.

1. **Larga distancia:** estas son utilizadas para distancias grandes, como puede ser a otra ciudad u otro país.
2. **Corta distancia:** son utilizadas para un mismo edificio o a varios edificios cercanos no muy retirados.

II.7.3. Tipos de Redes

Según su cobertura, se pueden clasificar en diferentes tipos:

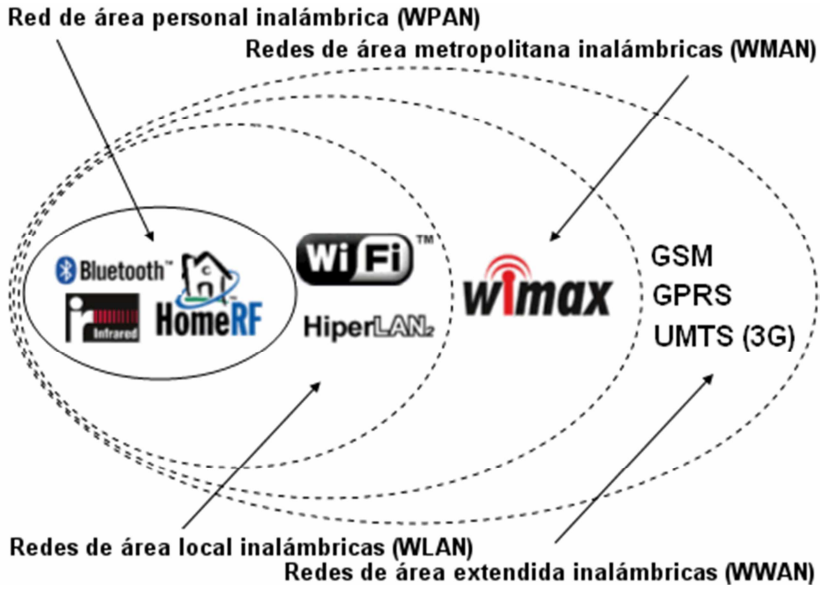

Figura II.4 Tipos de Redes

II.7.3.1. Wireless Personal Area Network

En este tipo de red de cobertura personal, existen tecnologías basadas en *HomeRF* (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores

mediante un aparato central); *Bluetooth* (protocolo que sigue la especificación IEEE 802.15.1); *ZigBee* (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); *RFID* (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto, similar a un número de serie único) mediante ondas de radio.

II.7.3.2. Wireless Local Area Network

En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HIPERLAN (del inglés, *High Performance Radio LAN*), un estándar del grupo ETSI, o tecnologías basadas en WiFi, que siguen el estándar IEEE 802.11 con diferentes variantes.

II.7.3.3. Wireless Metropolitan Area Network

Para redes de área metropolitana se encuentran tecnologías basadas en WiMAX (*Worldwide Interoperability for Microwave Access*, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a WiFi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (*Local Multipoint Distribution Service*).

II.7.3.4. Wireless Wide Area Network

Una WWAN difiere de una WLAN (wireless local area network) en que usa tecnologías de red celular de comunicaciones móviles como: WiMAX (aunque se aplica mejor a Redes WMAN), UMTS (*Universal Mobile Telecommunications System*), GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSPA y 3G, para transferir los datos. También incluye LMDS y WiFi autónoma para conectar a internet.

II.7.4. Características

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión pueden ser: las ondas de radio, las microondas terrestres o por satélite y los infrarrojos. Por ejemplo, dependiendo del medio, la red inalámbrica tendrá unas características u otras:

a) **Ondas de radio:** las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de los 300 a los 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 - 3000000000 Hz.

b) **Microondas terrestres:** se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante, ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

c) **Microondas por satélite:** se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia se mezclan bastante, así que pueden haber interferencias con las comunicaciones en determinadas frecuencias.

d) **Infrarrojos:** se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

II.7.5. Aplicaciones

Las bandas más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF (comunicaciones en navegación y submarinos), LF (radio AM de onda larga), MF (radio AM de onda media), HF (radio AM de onda corta), VHF (radio FM y TV), UHF (TV). Mediante las microondas terrestres, existen diferentes aplicaciones basadas en protocolos como *Bluetooth* o *ZigBee* para interconectar ordenadores portátiles, PDAs, teléfonos u otros aparatos. También se utilizan las microondas para comunicaciones con radares (detección de velocidad u otras características de objetos remotos) y para la televisión digital terrestre. Las microondas por satélite se usan para la difusión de televisión por satélite, transmisión telefónica a larga distancia y en redes privadas.

II.8. La IEEE (Institute of Electrical and Electronics Engineers) [18], [19]

II.8.1. Definición

IEEE corresponde a las siglas de (Institute of Electrical and Electronics Engineers) *Instituto de Ingenieros Eléctricos y Electrónicos*, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional, sin ánimo de lucro, formada por profesionales de las nuevas tecnologías, como: ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, matemáticos aplicados, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en Mecatrónica.

El IEEE abarca los campos de las ciencias de la computación, la tecnología biomédica, las telecomunicaciones, la ingeniería de potencia eléctrica, electrónica de potencia, sistemas de control, robótica y automatización, ingeniería en medicina y biología, educación, ingeniería de gerencia, etc. El IEEE es el mayor distribuidor de información

técnica en el mundo, produce casi el 30% de la literatura técnica publicada en electricidad, electrónica, e informática, convirtiéndose en el medio más eficiente para estar al día en el conocimiento de los últimos desarrollos técnicos en las áreas mencionadas.

II.9. WiFi Alliance [20], [21]

Es una organización creada por líderes proveedores de software y equipos inalámbricos con la misión de certificar los productos basados en el estándar 802.11 para lograr interoperabilidad y promover el término WiFi como una marca global para cualquier producto basado en el estándar 802.11.

Todos los productos basados en el estándar 802.11 son llamados WiFi, pero sólo los productos que han sido aprobados por la WiFi Alliance tienen permitido llevar la marca registrada "WiFi Certified". Antiguamente el grupo era conocido como WECA, pero cambió su nombre en octubre de 2002.

II.10. Tecnología WiFi [22], [23], [24]

II.10.1. Definición

La tecnología **WiFi (Wireless Fidelity**), ofrece la posibilidad de conexiones rápidas a través de señales de radio sin cables o enchufes. Las tecnologías: Bluetooth, WiFi, PDAs, WiMAX (WiFi de banda ancha), tienen el denominador común de referirse a tecnologías que permiten la comunicación de voz y datos sin utilizar cables. Estas tecnologías (tecnologías wireless) están reemplazando a los cables de conexión.

Esta nueva tecnología surgió por la necesidad de establecer, un mecanismo de conexión inalámbrico que fuera compatible entre los distintos aparatos. En busca de esa compatibilidad, fue que en 1999 las empresas: 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies, se reunieron para crear la Wireless Ethernet Compability Aliance (WECA), actualmente llamada WiFi Alliance. **WiFi** es una marca de la *WiFi Alliance* (anteriormente la *WECA: Wireless Ethernet*

Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

II.10.2. El nombre WiFi

Aunque se tiende a creer que el término WiFi es una abreviatura de *Wide Fidelity* (Amplia Fidelidad), la WECA contrató a una empresa de publicidad para que le diera un nombre a su estándar, de tal manera que fuera fácil de identificar y recordar. *Phil Belanger,* miembro fundador de WiFi Alliance que apoyó el nombre WiFi escribió:

"WiFi" y el "Style logo" del Ying Yang fueron inventados por la agencia Interbrand. Nosotros (WiFi Alliance) contratamos Interbrand para que nos hiciera un logotipo y un nombre que fuera corto, tuviera mercado y fuera fácil de recordar. Necesitábamos algo que fuera algo más llamativo que "IEEE 802.11b de Secuencia Directa".

II.10.3. Ventajas y desventajas

Las redes WiFi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas, porque cualquiera que tenga acceso a la red, puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes WiFi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.
- La WiFi Alliance asegura que la compatibilidad entre dispositivos con la marca *WiFi* es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología WiFi con una compatibilidad total.

Pero como red inalámbrica, la tecnología WiFi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema WiFi es una menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede causar.
- La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta WiFi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente *fáciles de conseguir* con este sistema.

La WiFi allience arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos muchas compañías no permiten a sus empleados tener una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista.
Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

II.11. Estándar WiFi IEEE 802.11 [25]

El estándar IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC del estándar 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red WiFi de una red Ethernet, es en cómo se transmiten las tramas o paquetes de datos. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet). El estándar 'IEEE 802.11' define el uso de los dos niveles inferiores de la arquitectura *OSI* (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

El IEEE 802.11 puede considerarse para “Ethernet inalámbrica”. El estándar original IEEE 802.11 lanzado en 1997 especifica CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance –Acceso Múltiple por Detección de Portadora/Limitación de Colisiones) como método de acceso al medio, parecido al utilizado por Ethernet. Todas las enmiendas del IEEE 802.11 son basadas en el mismo método de acceso.

Sin embargo, CSMA/CA, es un método de acceso muy ineficaz, puesto que sacrifica ancho de banda para asegurar una transmisión confiable de los datos. Esta limitación es inherente a todas las tecnologías basadas CSMA, incluyendo la CSMA/CD utilizada en Ethernet.

II.11.1. Aspectos técnicos

El estándar 802.11 para redes LAN inalámbricas incluye una serie de enmiendas. Las enmiendas contemplan principalmente las técnicas de modulación, gama de frecuencia y la calidad del servicio (QoS). Como todos los estándares 802 del IEEE, el IEEE 802.11 cubre las primeras dos capas del modelo de OSI (Open Systems Interconnection), es decir la capa física (L1) y la capa de enlace (L2).

Capa de enlace de datos (MAC)	802.2
	802.11
Capa física (PHY)	DSSS FHSS Infrarrojo

Tabla II.2 Aspectos Técnicos

Cualquier protocolo de nivel superior, puede utilizarse en una red inalámbrica WiFi, de la misma manera que puede utilizarse en una red Ethernet. La sección siguiente describirá lo que implica cada una de esas capas en términos de estándares inalámbricos.

II.11.1.1. Capa 1 (802.11 PHY)

La capa física tiene como finalidad, transportar correctamente la señal que corresponde a 0 y 1 de los datos que el transmisor desea enviar al receptor. Esta capa se encarga principalmente de la modulación y codificación de los datos.

Técnicas de modulación

Un aspecto importante que influencia la transferencia de datos, es la técnica de modulación elegida. A medida que los datos se codifican más eficientemente, se logran tasas o flujos de bits mayores dentro del mismo ancho de banda, pero se requiere *hardware* más sofisticado para manejar la modulación y la desmodulación de los datos.
La idea básica detrás de las diversas técnicas de modulación usadas en IEEE 802.11, es utilizar más ancho de banda del mínimo necesario, para mandar un "bit", a fin de conseguir protección contra la interferencia. La manera de esparcir la información conduce a diversas técnicas de modulación. Las más comunes de estas técnicas son:

- FHSS (Frequency Hopping Spread Spectrum –espectro esparcido por salto de frecuencia)
- DSSS (Direct Sequence Spread Spectrum –espectro esparcido por secuencia directa)
- OFDM (Orthogonal Frequency-Division Multiplexing –modulación por división de frecuencias ortogonales)

Frecuencia

Los estándares 802.11b y la 802.11g usan la banda de los 2,4 GHz ISM (Industrial, Científica y Médica) definida por la UIT. Los límites exactos de esta banda dependen de las regulaciones de cada país, pero el intervalo más comúnmente aceptado es de 2.400 a 2. 483,5 MHz. El estándar 802.11a usa la banda de los 5 GHz UNII (Unlicensed-National Information Infrastructure) cubriendo 5.15-5.35 GHz y 5.725-5.825 GHz en EEUU. En otros países la banda permitida varía, aunque la UIT ha instado a todos los países para que vayan autorizando la utilización de todas estas gamas de frecuencias para redes inalámbricas. La banda sin licencia de los 2.4 GHz, se volvió últimamente

muy “ruidosa” en áreas urbanas, debido a la alta penetración de las WLAN y otros dispositivos que utilizan el mismo rango de frecuencia, tal como: hornos de microondas, teléfonos inalámbricos y dispositivos Bluetooth. La banda de los 5 GHz tiene la ventaja de tener menos interferencia, pero presenta otros problemas debido a su naturaleza.

Las ondas de alta frecuencia son más sensibles a la absorción que las ondas de baja frecuencia. Las ondas en el rango de los 5 GHz son especialmente sensibles al agua, a los edificios circundantes u otros objetos, debido a la alta absorción en este rango. Esto significa que una red 802.11a, es más restrictiva en cuanto a la línea de la vista y se requieren más puntos de acceso para cubrir la misma área que una red 802.11b. Para la misma potencia de transmisión las celdas resultantes son más pequeñas.

II.11.1.2. Capa 2 (802.11 MAC)

La capa de transmisión de datos de 802.11, se compone de dos partes:

1. Control de acceso al medio (MAC)
2. Control lógico del enlace (LLC)

La subcapa LLC de 802.11 es idéntica a la de 802.2 permitiendo una compatibilidad con cualquier otra red 802, mientras que la subcapa MAC presenta cambios sustanciales para adecuarla al medio inalámbrico.

La subcapa MAC (L2) es común para varios de los estándares 802.11, y sustituye al estándar 802.3 (CSMA/CD – Ethernet) utilizado en redes cableadas, con funcionalidades específicas para radio (los errores de trasmisión son más frecuentes que en los medios de cobre), como fragmentación, control de error (CRC-Cyclic Redundancy Check), las retransmisiones de tramas y acuse de recibo, que en las redes cableadas son responsabilidad de las capas superiores.

Método de acceso al medio

El protocolo de acceso al medio en redes Ethernet cableadas, es el CSMA/CD, basado en la detección de colisiones y la subsiguiente retransmisión cuando éstas ocurren. En redes inalámbricas que utilizan la misma frecuencia para transmitir y recibir, es imposible detectar las colisiones en el medio, por lo que el mecanismo de compartición del medio, se modifica tratando de limitar las colisiones y usando acuse de recibo (ACK) para indicar la recepción exitosa de una trama.

Si el transmisor no recibe el ACK dentro de un tiempo preestablecido, supone que la transmisión no fue exitosa y la reenvía. Este protocolo se conoce como CSMA/CA, donde CA se refiere a "Collision Avoidance", es decir, tratar de evitar las colisiones. Este método no es tan eficiente como el CSMA/CD porque hay que esperar el ACK antes de poder continuar utilizando el canal y el mismo ACK consume tiempo de transmisión.

II.11.2. Estándares que certifica WiFi

Existen diversos tipos de WiFi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. Los siguientes estándares son:

II.11.2.1. 802.11a

La revisión 802.11a fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras *orthogonal frequency-division multiplexing* (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s

II.11.2.2. 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de

2,4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es, de aproximadamente 5,9 Mbit/s sobre TCP y 7,1 Mbit/s sobre UDP.

II.11.2.3. 802.11c

Es menos usado que los primeros dos, pero por la implementación que este estándar refleja. El estándar 802.11c es utilizado para la comunicación de dos redes distintas o de diferentes tipos, así como puede ser tanto conectar dos edificios distantes el uno con el otro, así como conectar dos redes de diferente tipo a través de una conexión inalámbrica. "El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI)".

II.11.2.4. 802.11d

Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

II.11.2.5. 802.11e

La especificación IEEE 802.11e ofrece un estándar inalámbrico que permite interoperar entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. A diferencia de otras iniciativas de conectividad sin cables, ésta puede considerarse como uno de los primeros estándares inalámbricos que permite trabajar en entornos domésticos y empresariales.

La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos. Estas prestaciones resultan fundamentales para las redes domésticas y para que los operadores

y proveedores de servicios conformen ofertas avanzadas. El sistema de gestión centralizado integrado en QoS evita la colisión y cuellos de botella, mejorando la capacidad de entrega en tiempo crítico de las cargas. Con el estándar 802.11, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de ***Calidad de Servicio (QoS*)** proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado *Hybrid Coordination Function (HCF)* con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access, equivalente a DCF.
- (HCCA) HCF Controlled Access, equivalente a PCF.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

- Background (AC_BK)
- Best Effort (AC_BE)
- Video (AC_VI)
- Voice (AC_VO)

II.11.2.6. 802.11f

Es una recomendación para proveedores de puntos de acceso, que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante, cambiarse claramente de un punto de acceso a otro mientras está en movimiento, sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como *itinerancia.*

II.11.2.7. 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Que es la evolución del estándar 802.11b, Este utiliza la banda de 2,4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares

II.11.2.8. 802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 802.11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radar o Satélite.

El desarrollo del 802.11h, sigue unas recomendaciones hechas por la ITU, que fueron motivadas principalmente, a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ECC/DEC/(04)08). Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

II.11.2.9. 802.11i

Está dirigido a batir la vulnerabilidad actual, en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales) y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

II.11.2.10. 802.11j

Es equivalente al 802.11h, en la regulación Japonesa

II.11.2.11. 802.11k

Permite a los conmutadores y puntos de acceso inalámbricos, calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN, mejorando así su gestión. Está diseñado para ser implementado en software y para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

II.11.2.12. 802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 300 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores) y debería ser hasta 10 veces más rápida, que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida, que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología *MIMO Multiple Input – Multiple Output,* que permite utilizar varios canales a la vez, para enviar y recibir datos gracias a la incorporación de varias antenas. El estándar 802.11n fue ratificado por la organización IEEE, el 11 de septiembre de 2009, con una velocidad de 600 Mbps en capa física.

II.11.2.13. 802.11p

Este estándar opera en el espectro de frecuencias de 5,9 GHz, especialmente indicado para automóviles. Será la base de las comunicaciones dedicadas de corto alcance (DSRC) en Norteamérica. La tecnología DSRC permitirá el intercambio de datos entre vehículos y entre automóviles e infraestructuras en carretera.

II.11.2.14. 802.11r

También se conoce como *Fast Basic Service Set Transition* y su principal característica es, permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso, antes de que abandone el actual y se pase a él. Esta función que una vez enunciada, parece obvia e indispensable en un sistema de datos inalámbricos, permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud, es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

II.11.2.15. 802.11s

Define la interoperabilidad de fabricantes en cuanto a protocolos *Mesh* (son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura.). Bien es sabido que no existe un estándar y que por eso, cada fabricante tiene sus propios mecanismos de generación de mallas.

II.11.2.16. 802.11v

IEEE 802.11v servirá para permitir la configuración remota de los dispositivos cliente. Esto permitirá una gestión de las estaciones de forma centralizada (similar a una red celular) o distribuida, a través de un mecanismo de capa 2. Esto incluye, por ejemplo, la capacidad de la red para supervisar, configurar y actualizar las estaciones cliente. Además de la mejora de la gestión, las nuevas capacidades proporcionadas por el 11v se desglosan en cuatro categorías:

- Mecanismos de ahorro de energía con dispositivos de mano VoIP WiFi en mente.
- Posicionamiento, para proporcionar nuevos servicios dependientes de la ubicación.
- Temporización, para soportar aplicaciones que requieren un calibrado muy preciso.
- Coexistencia, que reúne mecanismos para reducir la interferencia entre diferentes tecnologías en un mismo dispositivo.

II.11.2.17. 802.11w

Todavía no concluido. TGw está trabajando en mejorar la capa del control de acceso del medio de IEEE 802.11, para aumentar la seguridad de los protocolos de autenticación y codificación. Las LANs inalámbricas envían la información del sistema en tramas desprotegidas, que los hace vulnerables. Este estándar podrá proteger las redes contra la interrupción, causada por los sistemas malévolos que crean peticiones desasociadas, que parecen ser enviadas por el equipo válido. Se intenta extender la protección que aporta el estándar 802.11i, más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red. Estas extensiones tendrán interacciones con IEEE 802.11r e IEEE 802.11u.

II.11.2.18. 802.11y

Este estándar publicado en noviembre de 2008, permite operar en la banda de 3650 a 3700 MHz (excepto cuando pueda interferir con una estación terrestre de comunicaciones por satélite) en EEUU, aunque otras bandas en diferentes dominios reguladores también se están estudiando. Las normas FCC para la banda de 3650 MHz, permiten que las estaciones registradas operen a una potencia mucho mayor que en las tradicionales bandas ISM (hasta 20 W PIRE). Otros tres conceptos se añaden:

- *Contention Base Protocol (CBP)*
- *Extended Channel Switch Announcement (ECSA)*
- *Dependent Station Enablement (DSE)*

CBP incluye mejoras en los mecanismos de detección de portadora. ECSA proporciona un mecanismo para que los puntos de acceso (APs), notifiquen a las estaciones conectadas a él, de su intención de cambiar de canal o ancho de banda. Por último, la DSE se utiliza para la gestión de licencias.

II.12. Topologías WiFi [26], [27], [28]

II.12.1. Arquitectura general

En las redes WiFi, siempre existe como estructura básica, un gestor de la comunicación y una serie de clientes. Los clientes escucharán siempre para detectar la presencia de uno o más gestores, que les indicarán, entre otros datos, el nombre de la red que gestionan, el canal a usar, la seguridad y algoritmos de autentificación disponibles, etc. En base a esta información y la configuración del dispositivo en cuestión, el cliente será capaz de unirse a la red adecuada. Dependiendo de quién implemente la función de gestión de la red, nos encontraremos ante una red "*ad hoc*", en la que el gestor es un ordenador integrante de la propia red, o una red de tipo "*infraestructura*" en la que el gestor en un *access point*, *router* o similar.

II.12.2. Topologías lógicas

II.12.2.1. Topología IBSS (Independent Basic Service Set) o Ad Hoc

En el modo *ad hoc* los equipos cliente inalámbrico, se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente. La configuración que forman las estaciones se llama, conjunto de servicio básico independiente o IBSS. Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala, intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura. En una red ad hoc, el rango del BSS independiente está determinado por el rango de cada estación.

Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "*ver*" otras estaciones. A diferencia del modo *infraestructura,* el modo *ad hoc* no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida. En las redes "*ad hoc*" uno de los ordenadores realizará las funciones de gestor.

Lo cual indica que dicho ordenador ha de estar siempre funcionando o la red desaparecerá con él. Así mismo su localización ha de ser tal, que todos los demás miembros de esa red tengan "visibilidad radio" con él. Puede suceder incluso, que más de un ordenador asuma el rol de gestor, bien por un error de configuración, o porque alguno está configurado de forma que, cuando el gestor falle tome el control de la red y en caso de que este gestor de reserva y el gestor activo no se detecten, aparecerían dos gestores y por tanto dos redes, con clientes asociados a cada una de ellas, dependiendo de la cercanía al gestor que controla la celda y sin comunicación entre los dos grupos.

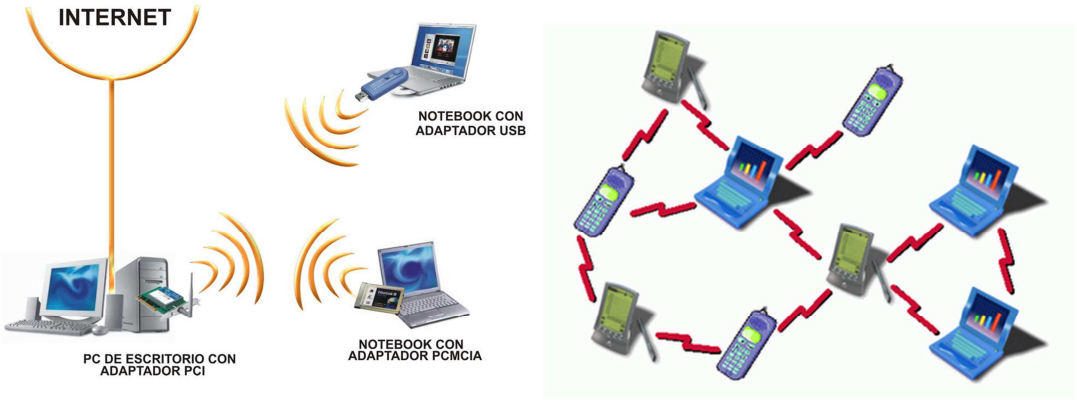

Figura II.5 Topologías Lógicas

En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles, estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

II.12.12.2. Topología BSS (Basic Service Set) o Infraestructura

En el modo de *infraestructura*, cada estación informática (abreviado EST) se conecta a un *access point* a través de un enlace inalámbrico. La configuración formada por el *access point* y las estaciones ubicadas dentro del área de cobertura, se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS), que es un identificador de 6 bytes (48 bits). En el modo

infraestructura el BSSID corresponde al *access point* de la dirección MAC.

Es posible vincular varios puntos de Access juntos (o con más exactitud, varios BSS), con una conexión llamada sistema de distribución (o SD), para formar un conjunto de servicio extendido o ESS. Este modo permite vincular la red inalámbrica con la red cableada, ya que el AP actúa como bridge entre las dos redes. La existencia de varios APs conectados a un sistema de distribución, que puede ser una LAN cableada, es lo que denominamos EBSS (Extended Basic Service Set).

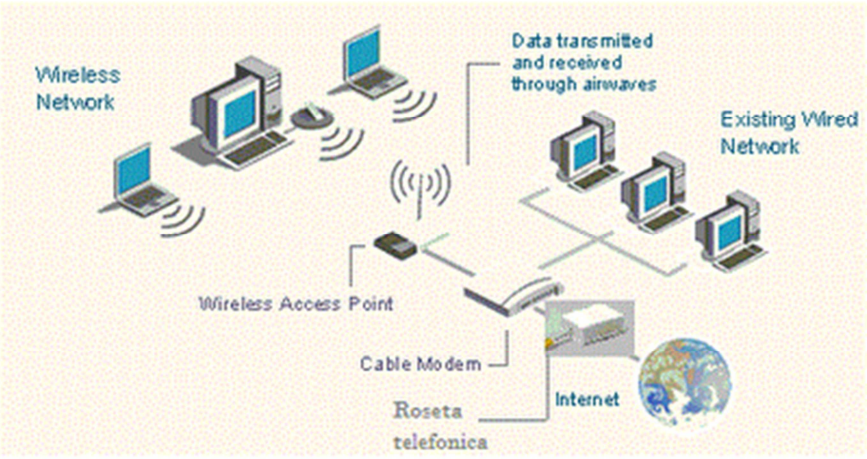

Figura II.6 Topología BSS

II.12.12.3. Topología híbrida

Esta topología combina la flexibilidad de ad hoc y la robustez de la infraestructura. Un WMN híbrido consiste de *routers Mesh* que conforman la espina dorsal de la red. Además, los clientes móviles pueden participar activamente en la creación del enmallado, proporcionando funcionalidades de red, tales como: enrutamiento y *forwarding* de paquetes de los datos.

Los clientes que ponen estas funcionalidades en ejecución, pueden por lo tanto actuar como extensión automática, a la pieza más estática de la infraestructura del enmallado. Las redes *Mesh* son muy flexibles y permiten combinar las ventajas de las arquitecturas

infraestructura y del cliente y en muchas ocasiones, la topología en malla, se utiliza junto con otras topologías para formar una topología híbrida.

II.12.12.4. Comparación entre redes Mesh y Ad hoc

La principal diferencia entre estas redes, es la movilidad de los nodos y la topología de red. La red *ad hoc* tiene una alta movilidad donde la topología de red cambia dinámicamente. Por otro lado están las redes *Mesh,* las cuales son relativamente estáticas con sus nodos fijos retransmitiendo. Por lo tanto, la movilidad de la red de WMN es muy baja en comparación con redes *ad hoc*. Respecto al funcionamiento del enrutamiento, las redes *ad hoc* son totalmente distribuidas, mientras que en las redes *Mesh* pueden ser total o parcialmente distribuido.

Por lo general las redes *ad hoc* son tenidas en cuenta para usos militares, mientras que las WMN se utilizan para ambos, usos militares y civiles. Algunos de los usos civiles populares de WMN incluyen el aprovisionamiento de los servicios del Internet en calles y ciudades. En esta topología no se requiere movilidad de puntos *Backhaul*, exceptuando el *roaming* de APs de RF o de otro tipo de puntos que cumplan con estas características. Las casas, comunidades, municipios y los negocios de pequeño y gran tamaño, son un ejemplo de redes en *infraestructura*. Sin embargo una red IP basada en una subred inalámbrica *ad hoc*, también denominada a veces red *Mesh*, está constituida por nodos de funcionalidad idéntica desde el punto de vista de la red, que se comunican entre sí a través de sus radios. No existe una infraestructura jerarquizada, de forma que cada nodo se coordina con los demás, como un igual a nivel de enlace y control de acceso al medio. Todos los nodos tienen funcionalidad completa de enrutadores IP y las comunicaciones extremo a extremo suceden por varios saltos (multihop), para lo cual se emplean habitualmente protocolos de enrutamiento dinámico, especialmente diseñados para este tipo de redes.

II.13. Elementos básicos para una red WiFi [29], [30]

Existen varios dispositivos WiFi, los cuales se pueden dividir en dos grupos:

- **Dispositivos de Distribución o Red**, entre los que destacan los *routers, access points* y repetidores.
- **Dispositivos Terminales,** que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

II.13.1. Dispositivos de Red

II.13.1.1 Router WiFi

Los *routers* inalámbricos, son dispositivos compuestos especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen: un *router* (encargado de interconectar redes), un *access point* y generalmente un *switch* que permite conectar algunos equipos vía cable. Su tarea es tomar la conexión a internet y brindar a través de ella, acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.

Figura II.7 Router WiFi

Características

- Permiten la conexión a la WLAN de dispositivos inalámbricos como: teléfonos celulares modernos, Netbooks, Laptops, PDAs, Notebooks y Access Points, para proveer de servicios de Internet.
- También cuentan con soporte para redes basadas en alambre (LAN - *Local Area Network*), esto es, tienen un puerto RJ45 que permite interconectarse con Switchs y

formar grandes redes entre dispositivos convencionales e inalámbricos, para su conexión a Internet.

- La tecnología de comunicación con que cuentan es a base de “ondas de radio”, capaces de traspasar muros, sin embargo ante cada obstáculo, esta señal pierde fuerza y se reduce su cobertura.
- Permiten la conexión ADSL (Asymmetric Digital Subscriber Line), la cual permite el manejo de Internet de banda ancha y ser distribuido hacia otras computadoras sin necesidad de cables e incluso hacia redes por medio de puerto RJ45.
- Cuentan con una antena externa, para la correcta emisión y recepción de ondas, así por ende, permite un correcto flujo de datos.

II.13.1.2. Access Points o Puntos de Acceso (APs)

Los puntos de acceso son dispositivos que generan un "set de servicio", que podría definirse como una "*red WiFi*" a la que se pueden conectar otros dispositivos. Los APs permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más APs a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal. El *Access Point* cubre una gran área inalámbrica entre ordenadores con dispositivos Wireless, realizando la función de receptor y emisor de señal, entre la red inalámbrica y la red cableada.

Figura II.8 Access Point

Sus funciones más importantes son:

- Ampliar la distancia inalámbrica entre los PCs Clientes inalámbricos y el receptor de señal o *access point.*
- Si nuestro *router* no tiene WLAN, el *access point* suple dicha función.
- Es un buen gestor de tráfico de la red inalámbrica, entre los terminales inalámbricos más próximos al *access point.*
- Pueden gestionar y controlar simultáneamente muchos ordenadores cliente a la vez, pudiendo llegar hasta 50 dispositivos simultáneos.
- El alcance es de unos 150 metros en zonas abiertas. En zonas amplias (+ de 150 metros) se necesitan más APs o Puntos de Extensión, para cubrir a todos los ordenadores inalámbricos de la red.

II.13.1.3. Puntos de Extensión Inalámbrica (EPs)

El Punto de Extensión (EPs), extiende el alcance de la red inalámbrica, retransmitiendo las señales de un ordenador o punto de acceso a otro punto de extensión. Los Puntos de Extensión no se conectan a la red Ethernet. La finalidad de los Puntos de Extensión, es encadenarse para pasar los datos entre Puntos de Acceso, Puntos de Extensión y ordenadores lejanos, de modo que se construye un puente entre ambos. Los metros que cubren dichos aparatos, van en función de los obstáculos (edificios, paredes, puertas) a sortear, pero lo normal son: 100 metros en interior y 300 metros en exterior.

Figura II.9 Punto de Extensión

Los Puntos de Extensión, tienen incorporado una tarjeta Ethernet para poder ser configurados vía navegador, pero no es necesario que sean conectados a la red inalámbrica, cuando ya están configurados y funcionando.

II.13.2. Dispositivos Terminales

II.13.2.1. Tarjeta PCI

Las tarjetas PCI para WiFi se agregan a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI, que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.

Figura II.10 Tarjeta PCI

II.13.2.2. Tarjetas PCMCIA

Las tarjetas PCMCIA, son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjetas inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas, solo son capaces de llegar hasta la tecnología b de WiFi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada.

Figura II.11 Tarjeta PCMCIA

II.13.2.3. Tarjetas USB

Las tarjetas USB para WiFi, son el tipo de tarjeta más común que existen en las tiendas y es la más sencilla de conectar a un PC, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse, incluso

tarjetas USB con el estándar 802.11N (Wireless-N), que es el último estándar liberado para redes inalámbricas.

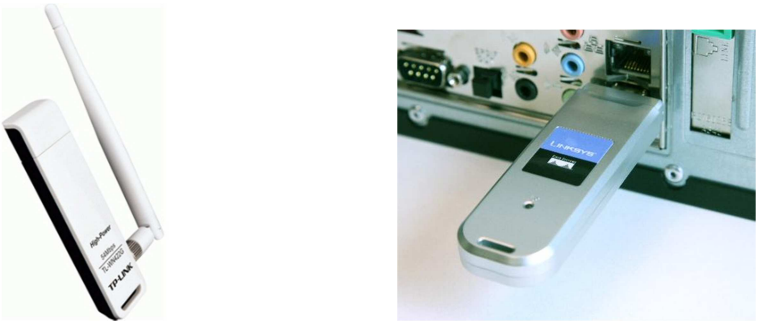

Figura II.12 Tarjeta USB

II.14. Frecuencias de transmisión WiFi [31], [32]

II.14.1. Frecuencias libres o no licenciadas

Se pueden definir como bandas no licenciadas de frecuencias, a aquellas, en las que se permite la operación de dispositivos de radiocomunicaciones, sin una planificación centralizada por parte de la Autoridad de Comunicaciones, es decir, sin una autorización individual de cada estación, tal que asegure la asignación de una frecuencia o canal para uso exclusivo de la misma.

La banda se destina íntegramente a tales dispositivos, sin subdivisión de canales, estableciéndose ciertos requerimientos básicos de convivencia, tales como: límites de potencia o de densidad de potencia radiada, anchura de banda mínima, etc.

La coordinación corre por cuenta de los usuarios, pero se apoya principalmente en la inmunidad contra interferencias, propia de la tecnología empleada y el modo de acceso múltiple a la banda. Las frecuencias no licenciadas, son una plataforma amplia, barata y rápida para construir soluciones inalámbricas. A pesar del gran uso del espectro de licencia libre, sigue siendo una excelente plataforma para construir enlaces inalámbricos de bajo precio, rápidos y confiables.

II.14.1.1. Bandas libres

La FCC ha proporcionado varias bandas de licencia libre (Bandas ISM & U-NII) para que puedan ser utilizadas por la comunidad inalámbrica:

- 900 MHz: 902-928 MHz
- 2.4 GHz: 2403-2483 MHz
- 5 GHz: 5725-5850 MHz, 5150-5250 MHz, 5250-5350 MHz, 5725-5825 MHz

Cuando la frecuencia se incrementa:

- Se vuelve más fácil de atenuar (no puede viajar tan fácil a través de obstáculos como copas de árboles, muros, etc).
- Capaz de transmitir mayor ancho de banda.

Cuando la frecuencia disminuye:

- Es más efectiva cuando transmite a través de obstáculos de menor atenuación (cuando es comparada con señales de frecuencias altas).
- No puede transmitir tanto ancho de banda, como alta sea la frecuencia de señal.
- Las bandas de frecuencias más bajas (900 MHz, 2.4GHz), están mucho más congestionadas, con más "tráfico" inalámbrico que las de frecuencia alta, como las bandas de 5GHz.

900 MHz vs 2.4 GHz vs 5 GHz Frecuencias Inalámbricas de Licencia Libre

	900 MHz	2.4 GHz	5 GHz
Popularidad	No usadas ampliamente por WISP	Ampliamente usadas	Volviéndose ampliamente usadas
Velocidad	Bajo Throughput	Alto Throughput	Alto Throughput
Costo	No caro	No caro	No caro
Frecuencia	Saturada	Saturada	No Saturada
Alcance	Alcance débil	Alcance promedio	Alcance promedio
Aplicación	Mesh, ptmp cortos con muchos obstáculos	Mesh, ptp, ptmp	Backhaul, ptp, ptmp

Tabla II.3 Frecuencias Inalambricas de Licencia Libre

II.15. Transmisión de la información WiFi (Flujo de datos) [33]

Los estándares 802.11a, 802.11b, 802.11g y 802.11n, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Estándar	Frecuencia	Velocidad	Rango
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi b (802.11b)	2,4 GHz	11 Mbit/s	100 m
WiFi g (802.11g)	2,4 GHz	54 Mbit/s	100 m
WiFi n (802.11n)	2,4 y 5 GHz	300 Mbit/s	100 m

Tabla II.4 Flujo de Datos

II.15.1. Estandar 802.11a

El estándar 802.11 tiene en teoría un flujo de datos máximo de 54 Mbps, cinco veces el del 802.11b y sólo un rango de treinta metros aproximadamente. El estándar 802.11a, se basa en la tecnología llamada OFDM (*multiplexación por división de frecuencias ortogonales*). Transmite en un rango de frecuencia de 5 GHz y utiliza 8 canales no superpuestos. Es por esto que los dispositivos 802.11a son incompatibles con los dispositivos 802.11b. Sin embargo, existen dispositivos que incorporan ambos chips, los 802.11a y los 802.11b y se llaman dispositivos de "*banda dual*".

Velocidad hipotética (en ambientes cerrados)	Rango
54 Mbit/s	10 m
48 Mbit/s	17 m
36 Mbit/s	25 m
24 Mbit/s	30 m
12 Mbit/s	50 m
6 Mbit/s	70 m

Tabla II.5 Estándar 802.11a

II.15.2. Estandar 802.11b

El estándar 802.11b permite un máximo de transferencia de datos de 11 Mbps, en un

rango de 100 metros aproximadamente en ambientes cerrados y de más de 200 metros al aire libre (o incluso más que eso con el uso de antenas direccionales).

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
11 Mbit/s	50 m	200 m
5,5 Mbit/s	75 m	300 m
2 Mbit/s	100 m	400 m
1 Mbit/s	150 m	500 m

Tabla II.6 Estándar 802.11b

II.15.3. Estandar 802.11g

El estándar 802.11g permite un máximo de transferencia de datos de 54 Mbps, en rangos comparables a los del estándar 802.11b. Además, debido a que el estándar 802.11g utiliza el rango de frecuencia de 2.4 GHz con codificación OFDM, es compatible con los dispositivos 802.11b con excepción de algunos dispositivos más antiguos.

Velocidad hipotética	Rango (en ambientes cerrados)	Rango (al aire libre)
54 Mbit/s	27 m	75 m
48 Mbit/s	29 m	100 m
36 Mbit/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

Tabla II.7 Estándar 802.11g

II.15.4. Estandar 802.11n

Es una propuesta de modificación al estándar IEEE 802.11-2007. Agregando Multiple-Input - Multiple-Output (MIMO) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC. También mejora significativamente el desempeño de la red más allá de los estándares anteriores, tales como 802.11b y

802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300 Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede transformarse en un desempeño visto por el usuario de 100Mbps. El estándar **802.11n**, hace uso simultáneo de ambas bandas 2.4 Ghz y 5 Ghz y de todos los Canales del Wifi a/b/g.

II.16. Pérdidas de Señal en WiFi (Interferencia WiFi) [34], [35]

II.16.1. Interferencia electromagnética

La interferencia electromagnética es la perturbación que ocurre en cualquier circuito, componente o sistema electrónico, causado por una fuente externa al mismo. También se conoce como **EMI** por sus siglas en inglés (Electro Magnetic Interference), Radio Frequency Interference o **RFI**. Esta perturbación puede interrumpir, degradar o limitar el rendimiento de ese sistema. La fuente de la interferencia puede ser cualquier objeto, ya sea artificial o natural, que posea corrientes eléctricas que varíen rápidamente, como un circuito eléctrico, el Sol o las auroras boreales. Las interferencias electromagnéticas se pueden clasificar en dos grupos:

- Intencionadas
- No intencionadas

El primer caso se refiere a interferencias causadas por señales emitidas intencionadamente, con el propósito expreso de producir una disfunción en la víctima, es decir, una interferencia. Entre las segundas se incluyen por un lado, aquellas causadas por señales emitidas con otra intención (generalmente sistemas de telecomunicaciones) y que accidentalmente, dan lugar a un efecto no deseado en un tercero; y por otro aquellas emitidas no intencionadamente (equipos electrónicos en su funcionamiento normal, sistemas de conmutación, descargas electrostáticas, equipos médicos, motores de inducción, etc).

Los obstáculos que causan interferencia pueden ser de tres tipos:

1 - Los que retienen la señal y que son inherentes a una casa (paredes, suelo, muebles, etc.). Cuanto menor es la cantidad de obstáculos que deba atravesar la señal, mayor es la cobertura.

2 - Los obstáculos que modifican la señal, son en su mayor número objetos metálicos (tal como es sabido por todos, los aparatos metálicos reflejan las ondas y las llenan de ruido). Cuanto más alejados de ellos, mejor será el alcance.

3 - Los que vampirizan las ondas y que son los aparatos que compiten por la señal (aquí englobamos a todos los aparatos inalámbricos que utilicen la misma frecuencia). Lo ideal es adquirir dispositivos inalámbricos que utilicen una frecuencia distinta a 2.4 Ghz.

Estándares

El CISPR (Comité Especial Internacional de Interferencia de Radio, por sus siglas en inglés) propone estándares para limitar la interferencia electromagnética radiada y conducida.

II.16.2. El CISPR [36]

El **Comité Internacional Especial de Perturbaciones Radioeléctricas** (*CISPR*, por sus siglas del idioma francés: *Comité international spécial des perturbations radioélectriques*). Es una organización de normalización, en el campo de las interferencias electromagnéticas en dispositivos eléctricos y electrónicos. Depende parcialmente de la Comisión Electrotécnica Internacional (IEC).

II.16.3. Interferencias WiFi [37]

En los últimos diez años la tecnología 802.11 ha dado pasos considerables, volviéndose cada vez más rápida, más fuerte y más escalable. Pero hay un problema que aún persigue al WiFi: la confiabilidad. Nada es más frustrante para los administradores de red, que los usuarios quejándose del accidentado desempeño de WiFi, la cobertura irregular y la caída de las conexiones. Manejar un entorno WiFi que no se puede ver y que cambia

constantemente es un grave problema y las interferencias de radio frecuencia (RF) son las culpables.

La interferencia de RF puede ser generada, por casi cualquier dispositivo que emita una señal electromagnética, desde teléfonos inalámbricos con auriculares *Bluetooth,* hornos de microondas e incluso medidores inteligentes. Pero de lo que muchas empresas no se dan cuenta, es que la mayor fuente de interferencias WiFi es su propia red inalámbrica.
A diferencia del espectro con licencia, que dedica una franja del ancho de banda al mejor postor, el WiFi es un medio compartido que opera en la radio frecuencia sin licencia, dentro del rango de los 2.4GHz y los 5GHz.

El problema de la interferencia de RF, se exacerba por el nuevo estándar 802.11n. El 802.11n, normalmente utiliza múltiples ondas de radio dentro de un AP, para transmitir simultáneamente varios flujos de WiFi en diferentes direcciones y lograr así una conectividad más rápida. Pero ahora, todo lo malo puede duplicarse. Si una sola de estas señales encuentra interferencia, la capacidad de multiplexar el espacio o de enlazar canales, se elimina. Y precisamente, son esas dos características mencionadas las que permiten a la tecnología 802.11n, alcanzar tasas de transferencia notablemente superiores.

La interferencia puede dar lugar a:

- Una disminución del alcance inalámbrico entre dispositivos.
- Una disminución de la transferencia de datos a través de la red *Mesh.*
- Pérdida de conexión intermitente o completa.

II.16.3.1. Fuentes de interferencias

- Dispositivos *Bluetooth* o estación base WiFi.
- Ciertas fuentes eléctricas externas, como líneas de alta tensión.

- Teléfonos a 2,4 GHz. Un teléfono inalámbrico que funcione en este rango de frecuencia, podría provocar interferencias con los dispositivos y redes inalámbricos encendidos.
- Altavoces inalámbricos que funcionen en las bandas de 2,4 GHz.
- Cualquier otro dispositivo "*inalámbrico*" que funcione en las frecuencias de 2,4 GHz (cámaras, dispositivos inalámbricos cercanos, etc.).

La ubicación del dispositivo dentro de un edificio y los materiales de construcción utilizados, puede afectar a la conexión WiFi. La tabla que aparece a continuación muestra elementos comunes y su potencial para provocar interferencias.

Obstáculo	**Grado de Atenuación**	**Ejemplo**
Espacio abierto	Ninguno	Cafetería, patio
Madera	Bajo	Paredes interiores, particiones de oficina, puertas, suelos.
Yeso	Bajo	Paredes interiores (yeso antiguo menor que yeso nuevo)
Materiales sintéticos	Bajo	Particiones de oficinas.
Bloque de hormigón	Bajo	Paredes internas y externas
Asbesto	Bajo	Techos
Cristal	Bajo	Ventanas
Cristal metálico tintado	Bajo	Ventanas tintadas
Malla de alambre en Cristal	Medio	Puertas, particiones
Cuerpo humano	Medio	Grupo grande de gente
Agua	Medio	Madera húmeda, acuario
Ladrillos	Medio	Paredes interiores y exteriores, suelos.
Mármol	Medio	Paredes interiores y exteriores, suelos.
Papel	Alto	Rollo o apilamiento de papel almacenado
Hormigón	Alto	Suelos, paredes exteriores, pilares de soporte
Cristal antibalas	Alto	Zonas de seguridad
Materiales plateados	Muy alto	Espejos
Metal	Muy alto	Mesas, particiones de oficina,

		hormigón reforzado, ascensores.

Tabla II.8 Fuentes de Interferencia

II.16.3.2. Soluciones comunes para hacer frente a las interferencias

Tres soluciones populares para hacer frente a las interferencias de RF incluyen:

- La reducción de la tasa física (PHY).
- La disminución de la potencia de transmisión de los APs afectados.
- El cambio de asignación de canal del AP.

Si bien cada uno de estos puede ser útil en algún aspecto, ninguno de ellos aborda el problema fundamental de tratar directamente con la interferencia de RF.

II.16.3.2.1. La reducción de la tasa física (PHY)

La gran mayoría de puntos de acceso en el mercado, hoy en día, usan antenas de dos polos omnidireccionales. Estas antenas envían y reciben transmisiones por igual en todas las direcciones. Debido a que estas antenas transmiten y reciben exactamente lo mismo en todas las situaciones, cuando la interferencia surge, estos sistemas solo tienen una opción para combatirla.

Tienen que bajar la tasa física de transferencia de datos físicos, hasta que se alcance un nivel aceptable de pérdida de paquetes. Sin embargo, la reducción de la tasa de datos del AP, puede tener el efecto contrario a lo deseado. Los paquetes están ahora en el aire por más tiempo, lo que significa que hay una mayor posibilidad de perder los paquetes, ya que tardan más en ser recibidos, haciéndolos más susceptibles a la interferencia periódica. Esta solución es muy ineficaz y consecuentemente, todos los usuarios que comparten ese AP experimentan un rendimiento pobre.

II.16.3.2.2. La disminución de la potencia de transmisión de los AP afectados

Otro método común para el diseño de WiFi, es el de reducir la potencia de transmisión al

AP, para hacer un mejor uso del limitado número de canales. Al hacer esto, se reduce el número de dispositivos que comparten un AP, lo cual mejora el rendimiento. Pero bajar la potencia de transmisión, también disminuye la intensidad de la señal recibida por los clientes. Esto se traduce en una velocidad de datos inferior y en células más pequeñas de WiFi, lo cual puede crear agujeros de cobertura. Estos agujeros deben ser llenados con más *access points*. La adición de más *access points* crea más interferencia.

II.16.3.2.3. El cambio de asignación de canal del AP

Aunque el cambio de canal es una técnica útil para hacer frente a la interferencia, continua en una determinada frecuencia, la interferencia tiende a ser muy variable e intermitente. Con limitados canales para cambiar, esta técnica puede causar más problemas que soluciones.

Dentro de la frecuencia de 2,4GHz, la banda de WiFi más utilizada, solo hay tres canales sin interferencias. Incluso dentro de la banda de los 5GHz, solo existen cuatro canales amplios que no se sobreponen en los 40 MHz. Después de la eliminación de selección dinámica de frecuencias (DFS o Dynamic Frequency Selection), hay un mecanismo para permitir que los dispositivos no licenciados compartan el espectro con los sistemas de radar existentes.

El cambio de canal por parte de un AP, requiere clientes conectados que se disocian y se asocian de nuevo, provocando la interrupción de aplicaciones de voz y vídeo. El cambio de canal crea un efecto dominó, a medida que los APs vecinos cambian de canal para evitar interferencias de co-canal.

La interferencia de co-canal se crea cuando los dispositivos interfieren entre sí, utilizando el mismo canal o frecuencia de radio para transmitir y recibir señales WiFi. La solución de cambio de canal, tampoco toma en cuenta qué es lo mejor para el cliente. En estos escenarios, la interferencia se determina desde el punto de vista del AP.

II.17. Seguridad y fiabilidad WiFi [38]

Uno de los problemas a los cuales se enfrenta actualmente la tecnología WiFi, es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios y esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad WiFi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes, son instalados sin tener en consideración la seguridad, convirtiendo así sus redes, en redes abiertas (o completamente vulnerables a los crackers), sin proteger la información que por ellas circulan.

El mayor problema de seguridad de las redes WiFi, viene dado por su dispersión espacial. No está limitada a un área, a un cable o una fibra óptica, ni tienen puntos concretos de acceso o conexión, si no que se expande y es accesible desde cualquier punto dentro de su radio de cobertura. Esto hace muy vulnerables a las redes inalámbricas, pues la seguridad física de dichas redes es difícil de asegurar. La posibilidad del acceso o monitorización de los datos es una amenaza muy real. Es por esta razón que todos los equipos permiten la ***encriptación*** de las comunicaciones mediante diversos algoritmos, que permiten: tanto autenticar a los usuarios para evitar accesos no autorizados, así como evitar la captura del tráfico de la red por sistemas ajenos a esta. Añadido a esto, existe la posibilidad de la realización de ataques de denegación de servicio (DoS), tanto los clásicos, comunes a todas las redes, como específicos de las redes WiFi. Tanto, ataques reales a los distintos protocolos de autentificación, como terminales que no cumplan con los tiempos y reglas de acceso impuestas por las normas WiFi, pueden degradar o incluso parar totalmente el funcionamiento de una red WiFi.

Sin embargo existe otro peligro: la inclusión de un punto de acceso no autorizado en la red. Un atacante puede añadir un *access point* que anuncie el mismo nombre de red, confundiendo así a algunos clientes, que se podrán llegar a conectar a él, en vez de a la

red legal. Dependiendo de la elaboración de la suplantación, el cliente puede llegar a revelar datos y claves importantes.

Para minimizar el peligro que supone la implementación de una red inalámbrica, existen una serie de normas básicas a tener en cuenta, a la hora de configurar la red, tales como:

- *Cambiar las configuraciones por defecto*
- *Activar encriptación*
- *Uso de claves "fuertes"*
- *Desactivar el anuncio del nombre de red (SSID)*
- *Filtrados de direcciones MAC*
- *Uso de direcciones IP estáticas*
- *VLAN propia para la red WiFi*
- *Instalación de un Firewall*

Estas medidas por sí mismas, correctamente implementadas, proporcionan seguridad suficiente para entornos no sensibles. Sin embargo existe la posibilidad de aumentar la seguridad mediante técnicas avanzadas, parte de las cuales precisan de la participación de un controlador de puntos de acceso. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son: la utilización de protocolos de cifradode datos para los estándares WiFi como el WEP, el WPA, o el WPA2, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos.

II.17.1. Métodos de encriptación

Las redes WiFi incorporan la posibilidad de encriptar la comunicación. Es una práctica recomendable, ya que al ser un medio inalámbrico, de no hacerlo sería muy simple capturar el tráfico que por ella circula y por tanto la captura por personas no deseadas, de datos sensibles. A lo largo del desarrollo de las redes WiFi, han ido surgiendo diferentes métodos de *encriptación* de las comunicaciones. Evolución necesaria, pues los distintos

métodos han resultado ser vulnerables y ha sido necesario implementar algoritmos más seguros que solventan y los implementan, por lo que la solución adoptada será siempre un compromiso entre rendimiento y seguridad. Los métodos estándar disponibles se detallan a continuación.

II.17.1.1. WEP (Wired Equivalent Privacy) [39], [40]

WEP, acrónimo de ***Wired Equivalent Privacy*** o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP, es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación).

Comenzando en 2001, varias debilidades serias fueron identificadas por analistas criptográficos, como consecuencia, hoy en día una protección WEP puede ser violada con software fácilmente accesible en pocos minutos. A pesar de sus debilidades, WEP sigue siendo utilizado, ya que es a menudo la primera opción de seguridad que se presenta a los usuarios por las herramientas de configuración de los routers, aun cuando sólo proporciona un nivel de seguridad, que puede disuadir del uso sin autorización de una red privada, pero sin proporcionar verdadera protección. Fue desaprobado como un mecanismo de privacidad inalámbrico en 2004, pero todavía está documentado en el estándar actual.

II.17.1.2. WAP (WiFi Protected Access)[41], [42], [43]

WPA (*WiFi Protected Access*, Acceso Protegido WiFi) es un sistema para proteger las redes inalámbricas (WiFi); creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP. WPA implementa la mayoría del estándar IEEE 802.11i y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por " WiFi Alliance".

WPA, adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

II.17.1.2.1. Características de la Seguridad de WPA

Las siguientes opciones de seguridad se incluyen en el estándar WPA:

II.17.1.2.1.1. Autenticación de WPA

En el estándar WPA se requiere autenticación 802.1x. En el estándar 802.11, la autenticación 802.1x era opcional. En entornos sin una infraestructura de Servicio de usuario, de acceso telefónico de autenticación remota (RADIUS), WPA admite el uso de una clave compartida previamente. En los entornos con una infraestructura RADIUS, se admiten el Protocolo de autenticación extensible (EAP) y RADIUS.

II.17.1.2.1.2. Administración de claves WPA

Con 802.1x, volver a usar las claves de cifrado de unidifusión es opcional. Además, 802.11 y 802.1x no proporcionan ningún mecanismo para cambiar la clave de cifrado global utilizada para el tráfico de multidifusión y difusión. Con WPA es necesario volver a usar las claves de cifrado de unidifusión y globales. Para la clave de cifrado de

unidifusión, el protocolo de integridad de clave temporal (TKIP), cambia la clave para cada marco y el cambio se sincroniza entre el cliente inalámbrico y el punto de acceso inalámbrico (AP). Para la clave de cifrado global, WPA incluye una utilidad para que el punto de acceso inalámbrico anuncie la clave modificada a los clientes inalámbricos conectados.

II.17.1.3. WAP2 (WiFi Protected Access 2) [44], [45], [46]

WPA2 (*WiFi Protected Access 2* - Acceso Protegido WiFi 2) es un sistema para proteger las redes inalámbricas (WiFi); creado para corregir las vulnerabilidades detectadas en WPA. WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. El estándar 802.11i fue ratificado en junio de 2004.

La alianza WiFi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise. Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2, que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público.

II.17.1.3.1. Algoritmo AES (Advanced Encryption Standard)

Advanced Encryption Standard (**AES**), también conocido como **Rijndael** (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques, adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197), el 26 de noviembre de 2001, después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. El cifrador fue desarrollado por dos criptólogos belgas: Joan

Daemen y Vincent Rijmen, ambos estudiantes de la *Katholieke Universiteit Leuven* y enviado al proceso de selección AES bajo el nombre "Rijndael".

II.17.1.3.1.1. Encriptación AES

AES es una técnica de cifrado de clave simétrica, que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente. AES proporciona una encriptación segura y ha sido elegida por NIST como un Estándar de Proceso de Información Federal en noviembre del 2001 (FIPS-197) y en Junio del 2003 el Gobierno de EEUU (NSA), anunció que **AES** es lo suficientemente seguro para proteger la información clasificada hasta el nivel **ALTO SECRETO**, que es el nivel más alto de seguridad y que se definen como información que pudiera causar "daños excepcionalmente graves" a la seguridad nacional en caso de ser divulgada al público.

El algoritmo AES utiliza una de las tres fortalezas de clave de cifrado: una clave de encriptación (contraseña) de 128, 192, o 256- bits. Cada tamaño de la clave de cifrado, hace que el algoritmo se comporte ligeramente diferente, por lo que el aumento de tamaño de clave, no sólo ofrece un mayor número de bits con el que se pueden cifrar los datos, sino también aumentar la complejidad del algoritmo de cifrado.

II.17.2. Filtrado de direcciones MAC [47], [48], [49]

Todo *adaptador de red* (término genérico de la tarjeta de red) tiene su propia dirección física (que se denomina dirección MAC). Esta dirección está representada por 12 dígitos en formato hexadecimal, dividida en grupos de dos dígitos separados por guiones y es un número único utilizado para identificar un dispositivo en una red. Este identificador suele estar impreso en el propio dispositivo.

El método de Filtrado de Direcciones MAC/MAC Address, consiste en suministrar a cada Punto de Acceso Inalámbrico, un listado de las direcciones MAC de los equipos que están autorizados a conectarse a la red. De esta manera, los equipos que no figuren en la lista serán rechazados. Significa establecer un filtro, por el que sólo se pueden

conectar a los *routers* y Aps, aquellos equipos que tienen una dirección MAC registrada. Esta dirección es única para cada controladora de red que hay en el mundo.

Esta precaución algo restrictiva, le permite a la red limitar el acceso a un número dado de equipos. Sin embargo, esto no soluciona el problema de la seguridad en las transferencias de datos.

II.17.2.1. Desventajas del filtrado de direcciones MAC

1. Cada AP debe programarse manualmente y esto provoca, además de una gran carga de trabajo, frecuentes errores al introducir los números MAC. Cada nuevo usuario deberá ser dado de alta. Una de los grandes atractivos de las redes inalámbricas, es facilitar la movilidad de los usuarios. En este caso, si se cuenta con varios APs, significa que la lista de direcciones debe mantenerse cargada y actualizada en cada uno de ellos.
2. Si algún dispositivo (PC portátil, o PDA) es robado o extraviado, deberá darse de baja inmediatamente de todas las listas de todos los APs, pues el que tenga ese dispositivo, estará autorizado para entrar a nuestra red.
3. Las direcciones MAC pueden ser "capturadas" por algún posible intruso y luego con ese dato tener acceso libre a nuestros sistemas.
4. Los APs también pueden ser sustraídos con relativa facilidad y en ese caso dejaríamos expuesto todo nuestro sistema de seguridad.
5. Por último, evidentemente este método no cumple con el estándar 802.1x, pues no se autentica al usuario, sino a los dispositivos y tampoco se solucionan las debilidades "nativas" de la encriptación WEP (claves estáticas).

II.17.3. Seguridad mediante controlador de Access Points [50]

El uso de un controlador de *access points*, no solo facilita la gestión y mantenimiento de una red WiFi, si no que puede servir así mismo para aumentar su seguridad. Las posibilidades que proporciona un controlador, dependerán del fabricante y del modelo, pues no hay un estándar. Son algunas de las más interesantes:

- ***Firewall (cortafuegos):*** Es habitual que los controladores implementen funcionalidades de *firewall,* que permitan controlar el tráfico que pasa de la red cableada a la red WiFi, en base a direcciones de origen o destino, aplicaciones, servicios, etc. El *firewall* es también un elemento importante en la defensa ante ataques de denegación de servicio (DoS).
- ***Comunicación por túnel:*** Si se dispone de esta capacidad, el controlador creará un túnel con cada uno de los *access points*. Dentro de ese túnel (normalmente un encapsulamiento IP o SSL) se transmitirá el tráfico de los clientes desde el *access point* al controlador. Esto permite que los clientes WiFi, potencialmente inseguros, no tengan acceso a la red directamente, sino que todo el tráfico deberá pasar por el controlador, el cual según las políticas asignadas a cada tráfico, por la funcionalidad de *firewall* en éste incluida, denegará o permitirá el acceso a partes o toda la red.
- ***Gestión por usuario:*** En conjunción con un servidor de autentificación, ya sea este interno al controlador o a un servidor RADIUS externo, será posible asignar diferentes accesos a los usuarios en función de sus credenciales, de una manera más detallada y compleja, que si el proceso lo llevara a cabo el *access point*. Así pues, podrán asignarse a diversas redes, concederles accesos a diferentes servicios, etc.
- ***Gestión del ancho de banda:*** El controlador podrá ofrecer una funcionalidad por la cual regulará el ancho de banda disponible, en función de la aplicación o usuario que desee hacer uso de ella. Así pues, podrá favorecerse el tráfico de voz, sobre el de datos, evitando la saturación y bloqueo de la red WiFi por aplicaciones abusivas, como descargas de ficheros, o priorizar el tráfico de la dirección, con respecto a los empleados o alumnos.
- ***Localización espacial:*** Un controlador puede ofrecer un servicio de localización. Puesto que tiene control de los diferentes puntos de acceso, puede monitorizar los clientes y la potencia de recepción de estos por cada uno de los APs. Si el Controlador tiene conocimiento de la situación espacial de los APs, triangulando la posición con respecto a los distintos puntos de acceso, en base a la potencia recibida por estos, podrá obtener la posición del cliente. Aunque esta posición no sea

completamente exacta, sí será importante a la hora de localizar equipos, no solo para la gestión física de estos, si no para encontrar a los atacantes o intrusos de una red.

- ***Limitación física del alcance de la red:*** Aunque la propagación de la señal de radiofrecuencia, no se puede acotar de forma efectiva en el espacio, un controlador que disponga del servicio de localización, podrá denegar el acceso a la red, a aquellos equipos cuya red se encuentre fuera de los limites, de aquello que se le indique como zona de cobertura. Es de indicar que con este método, los clientes fuera de la zona de cobertura de la red, seguirán recibiendo la señal, con lo que podrían intentar otros medios de ataque a ésta, si la encriptación no es adecuada, pero no podrán conectarse a la red.

II.17.4. WIPS (Wireless Intrusion Prevention System) [51]

Un WIPS es un conjunto de equipos de red, que como su mismo nombre indica tienen como objetivo prevenir y detectar intrusiones en la red WiFi (las siglas significan: Sistema de Prevención de Intrusión Inalámbrica). Un sistema WIPS siempre se compone de tres parte lógicas: los sensores que recogerán los datos de la red, el servidor que recolectará los datos de los distintos sensores, los analizará y relacionará y la consola que utilizará el personal, encargado de la seguridad de la red para acceder a los datos y visualizar las alarmas. Estos tres bloques lógicos, no siempre están separados físicamente, pues es habitual que el servidor implemente un servidor Web, que sea el utilizado para acceder a sus datos y configuraciones a través de un navegador.

No siempre un WIPS es un sistema independiente, en algunos sistemas, esta funcionalidad esta incluida en el controlador de puntos de acceso, que hará la función de servidor, que en conjunción con los puntos de acceso, que harán las funciones de sensores, pueden llevar a cabo parte de las funciones que realizaría un WIPS dedicado. Un WIPS monitoriza el espectro radioeléctrico de la red WiFi, con el objeto de detectar ataques de diversa índole, como pueden ser:

- ***Puntos de acceso infiltrados:*** Uno de los ataques mas efectivos suele ser la infiltración de un punto de acceso, el cual puede asociar clientes de la red, obteniendo por tanto datos de estos, que transmitirán creyendo estar conectados a la red legal. También, en caso de conectarlo a la red cableada, puede ser un punto de entrada a la red de cualquier intruso, que podrá acceder a distancia y por tanto será difícil de localizar.
- ***Ataques de denegación de servicio (DoS):*** Puesto que monitoriza la actividad, es capaz de detectar un comportamiento inusual de los clientes, identificándolo, si es el caso, con ataques de denegación de servicio.
- ***Access Points mal configurados:*** Puede detectar conversaciones entre puntos de acceso y los clientes, sobre todo en el momento de la asociación y negociación de la encriptación a usar, detectando parámetros y configuraciones erróneas. Pero incluso de forma más temprana, mediante la información emitida en los paquetes de *beacon* puede avisar de fallos en la configuración de puntos de acceso.
- ***Clientes mal configurados:*** Un cliente cuyos intentos de conexión a la red sean denegados de forma repetitiva, será detectado como un fallo de configuración de dicho cliente, o dependiendo el caso, como el intento de conexión de un atacante, que, especialmente en los casos en que intente averiguar las claves de la red, mediante métodos de fuerza bruta, provocará muchos intentos de conexión denegados por la red.
- ***Conexiones no autorizadas:*** Si WIPS tiene una lista de los clientes autorizados, podrá detectar la conexión de los clientes no autorizados, ya sean meros intentos de conexión o clientes que han entrado con éxito en la red.
- ***Redes ad hoc:*** Es muchos escenarios, una red *ad hoc* es un punto de vulnerabilidad importante. La red gestionada del tipo infraestructura, puede disponer de diferentes mecanismos de protección, pero una red *ad hoc*, puede ser creada involuntariamente por un error de configuración, un troyano, etc., lo que crea un agujero de seguridad que puede tener consecuencias importantes.
- ***Mac spoofing:*** recibe este nombre el ataque que consiste en suplantar la dirección MAC de otro equipo. Esto, en el caso de una red WiFi, permite ganar el acceso a la

red, en aquellas que tengan implementada una autorización de clientes, basada en sus direcciones de red. Un WIPS podrá detectar dos señales diferentes con la misma dirección MAC, evidenciando este tipo de ataque.

- ***Ataques "evil twin"/"honeypot":*** Este tipo de ataques consiste en realizar un *phishing* de un *hotspot*, es decir, insertar un punto de acceso que muestra al usuario el mismo interfaz que mostraría un *hotspo*t. Como consecuencia de esto, el cliente no notará diferencia entre el punto de acceso legal y el insertado y procederá a hacer uso de este.
- ***Ataques "man-in-the-midle":*** Este es un tipo de ataque en el cual, el atacante se posiciona entre el cliente y el servicio que ha de utilizar. Así en una red WiFi, este ataque consistiría en que el cliente se conecta al sistema del atacante, gracias a algún engaño por parte de este, y el sistema del atacante a su vez reenvía los datos al punto de acceso legal. De esta forma el cliente no ser percatará de que no está conectado a la red directamente, pues todo parece funcionar perfectamente, pero el atacante tiene acceso a todos los datos del cliente, puesto que pasan por su sistema.

II.18. Sistemas de gestión WiFi centralizados [52]

Originalmente los sistemas WiFi eran autónomos. Cada punto de acceso tenía toda la capacidad para crear la celda y gestionar los clientes a ella asociados y las comunicaciones entre estos y entre ellos y la red cableada. Cuando las redes WiFi pasaron de ser una solución puntual para solventar problemas concretos y siempre de tamaño reducido, a grandes instalaciones complejas que soportan gran parte de las comunicaciones de una empresa, o incluso en algunos casos son en si mismo la fuente de ingresos, se vio la necesidad de disponer de sistemas de gestión centralizados.

La primera aparición de estos sistemas, vino dado por el alto precio de los puntos de acceso en sus primeros tiempos. Para abaratar las grandes instalaciones, se tomó la decisión de hacer puntos de accesos menos inteligentes y se transfirió esa inteligencia a un sistema centralizado. Es cierto que este sistema de control suele tener un coste elevado, pero si la instalación es grande, la reducción en el precio de cada punto de

acceso lo compensa y el precio global es mas reducido, que en el caso de una instalación realizada con puntos de acceso autónomos.

Con el tiempo, las redes WiFi fueron soportando más servicios y se demandó cada vez mas de ella, teniendo que aportar más opciones de configuración y funcionalidades que las hicieran aptas para las aplicaciones y servicios que de ellas hicieran uso. En instalaciones con un elevado número de puntos de acceso, la configuración manual de cada uno de ellos y su mantenimiento, así como la detección y corrección de errores, se tornó compleja y el coste en tiempo y personal demasiado elevado. Los sistemas de gestión centralizados tienen como objetivo disminuir estos problemas y ofrecer funcionalidades añadidas.

Dependiendo del fabricante, se implementarán distintas medidas para elegir que puntos de acceso han de ser gestionados, ya sea mediante una reconfiguración de la dirección IP en el punto de acceso, o mediante algún tipo de filtrado y/o clave en el controlador. Una vez añadido el punto de acceso, se le cargará automáticamente una configuración base, lo cual reduce los tiempos de instalación y minimiza los errores de configuración.

El objetivo general de esta fase es que la instalación de nuevos sistemas se simplifique. Una vez realizado el despliegue inicial, el controlador permitirá, desde una sola consola configurar los distintos puntos de acceso, individualmente, por grupos o globalmente, así como recibir alarmas asociadas al funcionamiento de ellos. La funcionalidad depende de cada fabricante, pero estas son algunas de las ofrecidas:

- ***Gestión centralizada:*** Una sola consola para gestionar los distintos puntos de acceso.
- ***Centralización de eventos:*** En instalaciones amplias, con un elevado número de puntos de acceso, resulta inviable acceder a cada uno de ellos para tener conocimiento de los eventos acontecidos y posteriormente relacionar los datos obtenidos de cada uno de ellos. El controlador permite automatizar este proceso con un ahorro en costes y un aumento en la fiabilidad de la red.

- ***Seguridad avanzada y centralizada:*** Permite gestionar la admisión de clientes WiFi, definir perfiles, permitir acceso de éstos a distintas partes de la red o servicios, dependiendo de su identidad, filtrado y detección de accesos, etc.
- ***Servicios de localización de clientes WiFi:*** Puesto que el sistema de gestión centralizada controla todos los puntos de acceso, es capaz de obtener los datos de potencia de recepción, que cada uno de ellos obtiene de cada uno de los clientes. En la siguiente imagen se muestra como con tres puntos de acceso, se puede deducir la distancia a ellos de una terminal, basándose en la potencia recibida, y con estas tres distancias, obtener la localización del cliente WiFi.

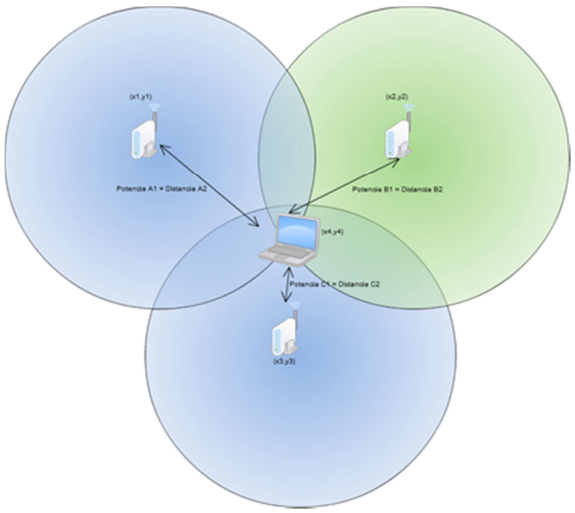

Figura II.13 Sistemas de gestión WiFi centralizado

- ***Autorización por localización:*** relacionado con el punto anterior, al tener conocimiento de la localización de los clientes, este servicio puede limitar el acceso a la red, solo a aquellos que se encuentren en las áreas permitidas.
- ***Respuesta automatizada ante fallos:*** Es posible, por ejemplo que ante el fallo de un punto de acceso, el controlador de forma automática active alguno que estuviera de reemplazo, o aumente la potencia de los circundantes para aumente su cobertura y cubrir el área que se quedó sin servicio.
- ***Gestión de la calidad de servicio:*** Puede priorizar, restringir o controlar el tráfico de ciertas aplicaciones, servicios o usuarios.

- ***Tunelización:*** Es posible ofrecer el servicio de que los datos de la red WiFi, no sean inyectados a la red cableada directamente por el punto de acceso, sino que se genere un túnel entre éste y el gestor centralizado. De esta manera se permite que el gestor pueda controlar los datos del cliente, realizando sobre ellos funciones como: priorización, filtrado y monitorización.
- ***Gestión de estructuras de red "Mesh":*** La incorporación de un gestor, permitirá la elección de forma automática de los enlaces atendiendo a la calidad de estos, de manera que, se optimicen los caminos y por tanto el rendimiento y fiabilidad. Además es posible que el gestor, ante el fallo de un punto de acceso o un enlace, recomponga de forma automática la arquitectura de la malla, de forma que la comunicación se mantenga.

II.19. Enlaces inalámbricos (WDS) [53]

Una funcionalidad ofrecida por muchos puntos de acceso, es la posibilidad de realizar enlaces inalámbricos entre dos de ellos, con el objetivo principal de unir dos redes y en algunos casos, para proporcionar cobertura inalámbrica en puntos donde no hay acceso a la red cableada, sin renunciar a la comunicación con esta. El sistema para realizar este tipo de enlace no esta estandarizado, existiendo multitud de soluciones propietarias, cada una con sus virtudes y defectos, aunque los principios básicos de funcionamiento son similares.

Sin embargo, hay un método de comunicación que aun no teniendo certificación de la WiFi Alliance, ni de ningún otro organismo, es ampliamente utilizado. Hay que tener en cuenta sin embargo, que al no tener ninguna certificación, los sistemas que utilicen este protocolo, no serán en la mayoría de los casos, compatibles entre si y en muchos, ni tan siquiera entre distintos modelos pertenecientes al mismo fabricante. El método referido es el *Wireless Distribution System (WDS).*

La meta de este protocolo, es permitir la interconexión de los puntos de acceso de una red 802.11, sin necesidad de estar conectados a una red cableada, preservando la dirección MAC (equivalente a la dirección Ethernet, cuando la trama llegue a la red cableada) de cada uno de los clientes. La conservación de la dirección MAC de los clientes, provoca que el enlace WDS, sea percibido por el resto de los equipos como un cable que no influye en la comunicación. En una red WDS, un punto de acceso puede ser configurado de manera que asuma uno de los siguientes tres roles:

- **Estación base principal**: Es el punto de acceso que está conectado a la red cableada. Podrá dar cobertura a clientes locales y aceptará conexiones de estaciones bases repetidoras o remotas.
- **Estación base repetidora**: Es aquella que recibe y tramita datos, ente una estación base remota u otra estación base repetidora y una estación base principal u otra estación base repetidora. Por tanto realizará saltos intermedios y como su propio nombre indica, repetirá la señal para alcanzar puntos más lejanos. Así mismo puede dar servicio a clientes inalámbricos locales.
- **Estación base remota**: Es aquella que da servicio a clientes locales y que tiene enlaces a estaciones base remotas, o estaciones base principales, pero no es un salto intermedio para otras estaciones base.

Dependiendo del fabricante, los puntos de acceso pueden tener la posibilidad de crear más de un enlace WDS, lo que les permitirá crear redes en malla "*Mesh*". Así mismo hay productos, que para evitar la pérdida de velocidad con cada salto, dotan a los mismos con dos módulos de radio, pudiendo utilizar el primero para crear el enlace con otras estaciones base y el segundo para dar cobertura local.

Como se puede ver por lo expuesto hasta ahora, las redes WDS pueden ser utilizadas en dos modos:

- ***Puente inalámbrico:*** En este modo el equipo no permite la conexión de clientes locales, no forma una celda de cobertura WiFi. Se utiliza para crear enlaces punto a punto, por ejemplo: entre edificios.

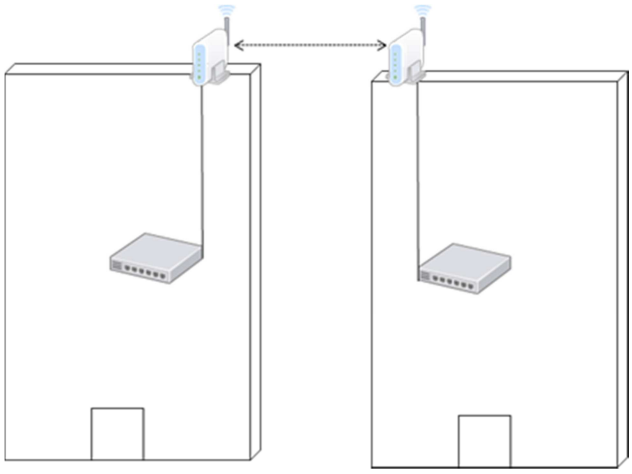

Figura II.14 Puente Inalámbrico

- ***Repetido inalámbrico:*** Con esta configuración el equipo, además de crear el enlace WDS con otras estaciones base, permite la conexión de clientes, creando una celda que será una extensión de la red WiFi.

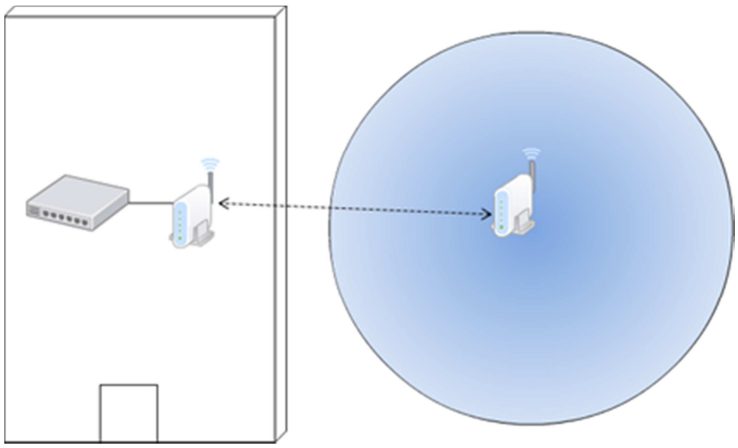

Figura II.15 Repetido Inalámbrico

Los enlaces WDS usualmente presentan limitaciones en el campo de la seguridad. No están disponibles todas las opciones de encriptación y en los equipos más económicos, solo los métodos más básicos de encriptación y autentificación están disponibles. Esto es

peligroso, puesto que lo normal, es que estos enlaces se efectúen a través de lugares públicos y espacios abiertos, porque son justamente estos espacios los que impiden el acceso a la red cableada y hace necesario un enlace inalámbrico. Así pues, si el equipo no implementa mecanismos fiables de encriptación, expondrá un punto de intrusión y ataque a la red.

II.20. **Roaming** [54], [55]

El *roaming* (o su traducción como *itinerancia*) es un concepto utilizado en comunicaciones inalámbricas, que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. El concepto de *roaming* utilizado en las redes WiFi, significa que el dispositivo WiFi del cliente, puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.

II.20.1. Roaming en redes WiFi

Para que sea posible, tiene que haber una pequeña superposición (*overlapping*) en las coberturas de los puntos de acceso (*Access Points*), de tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura. Los puntos de acceso incorporan un algoritmo, que decide cuándo una estación debe desconectarse de un punto de acceso y cuándo conectarse a otro. Ello permite, no sólo la conexión en diferentes puntos distantes en los que el cliente tiene servicio, sino también, que la conexión (WiFi) permanezca activa y no se interrumpa.

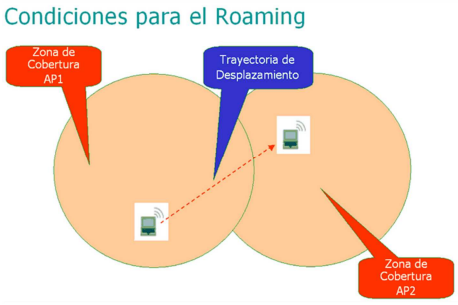

Figura II.16 Roaming en Redes WiFi

En la figura, vemos la zona de superposición y la trayectoria de desplazamiento indicada por la flecha y como es posible desplazarse de AP1 a AP2, sin perder la señal de WiFi. El usuario está conectado al comienzo AP 1 y en determinado momento pasa a recibir la señal del AP 2.

II.20.1.1. El Roaming y los Paquetes Beacons

Como vimos, los Puntos de Acceso Inalámbricos, emiten intermitentemente unos paquetes denominados ***Beacons***. Cuando una estación se aleja demasiado de un Access Point, "pierde la señal", es decir que deja de percibir estos *Beacons* que le indican la presencia del Access Point. Si hay superposición, se comienzan a captar los *Beacons* del otro Access Point, hacia el cual se está dirigiendo, a la vez que se van perdiendo gradualmente los del anterior.

II.20.1.2. El Roaming y los Paquetes ACK

También se vio, que una vez que se envía un paquete de datos en las redes inalámbricas WiFi, la estación receptora envía un "OK.", denominado **ACK**. Si la estación emisora se aleja demasiado de la transmisora, es decir que sale del radio de cobertura, no captará los ACK enviados. Los equipos de WiFi incorporan un algoritmo de decisión, que debe determinar en qué momento se desconectan del Access Point 1 y se conectan al Access Point 2, como se ve en la figura anterior.

II.20.2. La Problemática del Roaming

El estándar 802.11 WiFi, no contiene instrucciones detalladas sobre el tema del *roaming,* por lo tanto, cada fabricante diseña el algoritmo de decisión según su criterio y con los parámetros que estima convenientes. Por esta razón pueden existir problemas, sobre todo en grandes ambientes, al mezclar *access points* de diferentes fabricantes o *access points* de un mismo fabricante, con dispositivos móviles de otras marcas. Cada uno tendrá otro algoritmo de decisión y pueden producirse falencias en el *roaming.* También influye en esta decisión la sensibilidad del cliente RF, pues como vimos son casi todos diferentes.

II.21. Video, Voz y Datos en una red WiFi [56]

La mayor capacidad de las redes de datos y de los equipos, tanto ordenadores como sistemas especializados, así como su menor coste, ha hecho que se popularice el uso de tráfico multimedia. Actualmente es normal que las diferentes operadoras de telefonía, ofrezcan lo que se suele llamar "triple play", que designa el servicio de datos, voz y audio sobre redes IP. Este servicio se ha popularizado en las redes privadas, siendo habitual que conviva la voz sobre IP (VoIP) con los datos en la misma red, debido a las ventajas en funcionalidad y reducción de costes que ofrece sobre la telefonía convencional.

Recientemente el servicio de video se ha desarrollado notablemente, tanto a nivel particular, como empresarial y muy notablemente en centros de enseñanza, donde aporta nuevas posibilidades docentes. La transmisión de video y voz a través de una red IP convencional, presenta una serie de retos, debido a las necesidades específicas de este tipo de tráfico, que fuerzan a que los elementos de red, deban poseer ciertas características necesarias para el buen funcionamiento del servicio.

Si esto es cierto en redes cableadas, lo es mucho mas en redes WiFi, puesto que en este último caso, el medio es compartido, no solo con interferencias y elementos externos, sino con el resto de los clientes.

II.21.1. Necesidades del tráfico de datos

La transmisión de datos, como pueden ser: ficheros de un servidor, correo electrónico o páginas WEB, es un tráfico poco exigente. El servicio demanda la mayor velocidad de transmisión y la menor pérdida de paquetes posible. Es cierto que en las redes WiFi, estos dos parámetros, no son tan fáciles de optimizar como en las redes cableadas, pues las velocidades de transmisión son menores y siempre existe alguna interferencia externa, o simple colisión entre clientes, lo que provocará alguna perdida. El usuario lo que apreciará es la velocidad de acceso a los datos, pero a no ser que ésta se reduzca, por debajo de un cierto umbral que la haga inaceptable y ese umbral dependerá de la

aplicación, no habrá una mayor exigencia.

II.21.2. Necesidades del tráfico de video

El tráfico de video es más exigente. Con respecto a la transmisión de datos, este tipo de tráfico añade requerimientos extras, los cuales están motivados porque el video ha de ser mostrado en el instante que corresponda. El hecho de que los datos lleguen más despacio en una página web, influye en que tarde menos o más en bajar, pero los fotogramas del video se han de mostrar cuando correspondan, o el video no será visionado de forma correcta, apreciándose defectos, sonido deficiente, aceleraciones del vídeo, pausas, etc.

En general aparte de una velocidad de transmisión mínima, para poder transmitir en video con fiabilidad y una falta de pérdida de paquetes, hará falta el cumplimiento de otros parámetros como: el jitter, latencia, duplicación y reordenación de paquetes y emisión en ráfagas. El video, dependiendo de la codificación y la calidad de la imagen, demandará un ancho de banda mínimo, que deberá ser soportado por la red WiFi para proporcionar un buen servicio. En caso de que la red no sea capaz de proporcionar esta velocidad, se perderá información, al no poder ser enviada por la red, provocando pérdida de paquetes. La pérdida de paquetes, ya sea por causa de un tráfico excesivo para la red, por interferencias o cualquier otra causa, provocará videos de calidad deficiente, mostrándose los típicos cuadros y cortes de sonido.

II.21.3. Necesidades del tráfico de voz

Las necesidades del tráfico de voz, en este caso voz sobre IP (VoIP), son análogas a la del video, puesto que se trata de un servicio que no permite perdida de información y que precisa de una temporización muy estricta. Sin embargo, existen dos diferencias con respecto al servicio de video. La primera es, que aunque es necesario que se garantice un ancho de banda y que este dependerá del sistema de codificación de la voz que utilice el sistema, esta velocidad de transmisión será mucho menor que en el caso del video. La segunda diferencia a tener en cuenta es que la latencia, es un parámetro importante para la voz. Si esta es alta, la red no será apta para conversaciones de voz, pues un retraso

mínimo es percibido muy negativamente por los usuarios.

II.22. Calidad de servicios (QoS) en redes WiFi [57], [58]

II.22.1. Introduccion a QoS

QoS o **Calidad de Servicio** (*Quality of Service*, en inglés), son las tecnologías que garantizan, la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones, tales como la transmisión de vídeo o de voz. Puesto que cada servicio, cada tipo de tráfico, tiene unas necesidades diferentes, es preciso diferenciarlo y aplicarle un tratamiento individual acorde a sus requerimientos. La aplicación de políticas de QoS, no solo proporciona la posibilidad de ofrecer datos, voz y videos con calidad, si no que aporta herramientas para priorizar tráficos, ya sea por la naturaleza de éste (priorizar web, sobre el correo y todas sobre las transferencias de ficheros P2P), o por el origen (el tráfico de la dirección de un centro escolar, podrá ser priorizado sobre el de los alumnos). No basta con disponer de ancho de banda suficiente, pues un sistema que deba transmitir datos sensibles, como voz o video, debe de implementar necesariamente QoS. La razón es simple, si durante una transferencia de voz o video, se produce una descarga de datos, esta podría ocupar todo el ancho de banda disponible.

Sin embargo el problema no surge solo en ese caso, pues aunque la descarga de datos no demande la velocidad máxima de transferencia, emitirá tráfico y el dispositivo de red, en nuestro caso, el punto de acceso o el controlador de la red WiFi, deberá tener mecanismos para decir, que paquetes ha de emitir antes y/o con una cadencia fija, minimizando las pérdidas, la latencia, el jitter, las ráfagas, etc.

Para conseguir este objetivo y minimizar los problemas en la transmisión de contenido multimedia, existieron protocolos propietarios, pero en un entorno como el de las redes WiFi, donde es posible tener control sobre los puntos de acceso, pero no sobre los clientes, donde suelen convivir distintos dispositivos y de distintos fabricantes, no

resultaron funcionales ni se obtenían los resultados deseados. Fue con la llegada del protocolo 802.11e y su respaldo por parte de la WiFi Alliance, con su certificación *Wireless Multimedia Extension* (WME), más conocida como *WiFi MultiMedia* (WMM), cuando la QoS llegó al mundo WiFi.

II.22.2. 802.11e (WMM)

Por lo expuesto en el punto anterior, surgió la necesidad de tener algún mecanismo, no solo para que todos los clientes pudieran transmitir sus datos eficientemente, sino también para priorizar la transmisión de los datos sensibles, razón por la cual se desarrolló la norma 802.11e.

La norma 802.11e, clasifica el tráfico en cinco categorías, dependiendo de las necesidades y características del tráfico. Estas categorías, ordenadas de la más prioritaria a menos prioritaria son:

- **Voz (AC_VO):** A esta categoría pertenecerá el tráfico de Voz.
- **Video (AC_VI):** Categoría en la que se encuadrará el tráfico de video que necesite prioridad, lo cual, en principio, debería excluir al video Flash.
- **"Best Effort" (AC_BE):** Tráfico que deberá transmitirse tan pronto como sea posible, tras atender a aquel que le sea mas prioritario. Tráfico de este tipo podría ser una sesión Telnet o de control remoto de un equipo, que aunque no sea tan crítico como los anteriores, si será sensible a lentitud y perdidas, dando sensación al usuario de falta de respuesta.
- **"Background" (AC_BK):** Es el tráfico que no entra en ninguna de las otras categorías. Es el tráfico de fondo o de relleno, de aquellas aplicaciones que no necesitan un tratamiento especial, como pueden ser: correo electrónico, la trasferencia de ficheros o el acceso a páginas WEB.
- **"Legacy DCF":** Esta no es realmente una categoría contemplada en la norma 802.11e, pero aun así, es un grupo de tráfico que recibe un tratamiento diferente. Engloba a todo el tráfico que no tenga tratamiento prioritario, normalmente gestionado por equipos que no cumplen con la norma 802.11e y por tanto no se

engloba en ninguna de las categorías que la norma prevé. Por esta razón, al no tener indicación de la prioridad con que ha de ser tratado, será el menos prioritario de todos.

Esta norma amplía los sistemas de control existentes hasta el momento, DCF (*Distributed Coordination Function*) y PCF (*Point Coordination Function*), con un nuevo esquema denominado HCF (*Hybrid Coordination Function*), que define dos métodos de acceso al canal para la emisión de datos, priorizando aquellos que mas sensibles sean: *Enhanced Distributed Channel Access* (EDCA) y HCF *Controlled Channel Access* (HCCA). Ambos métodos tienen una base común, siendo el EDCA el más extendido y obligatorio para los sistemas certificados WiFi y que soporten WMM. El método HCCA incorpora un mayor control del tráfico, pero su cumplimiento es opcional y hoy en día esta menos extendido y es soportado por un número muy reducido de sistemas.

II.22.2.1. Enhanced Distributed Channel Access (EDCA)

Este método, de obligado cumplimiento para los equipos que posean la certificación WMM de la WiFi Aliance, se basa en la variación de los temporizadores, presentes en los controles estándar de las redes WiFi. Para comprender el funcionamiento, previamente será necesario conocer, los mecanismos que regulan el momento de transmisión de los clientes y su acceso al medio.

Añadido a la regulación impuesta por los controles DCF (que a su vez se compone de los controles CSMA/CA y RTS/CTS), existe una regularización en el momento de acceso a la red, principalmente orientado a evitar, la monopolización del canal por un terminal y minimizar el acceso simultáneo al canal de dos o más terminales.

Para ello, un cliente que ha transmitido datos, no podrá volver a transmitir hasta pasado un tiempo fijo, que recibe el nombre de: *Arbitration Inter-Frame Space* (AIFS).

Esta espera posibilita a otros sistemas tener la oportunidad de ocupar el canal y transmitir, pues de otra forma, una sola estación podría estar emitiendo continuamente, no dando opción a otra a hacerlo, pues siempre verían el canal ocupado y según el protocolo CSMA/CA, no podrían transmitir para evitar colisiones. Para minimizar la situación en que los terminales que deseen emitir, comprueben la ocupación del canal simultáneamente y emitan colisionando y lo que es mas importante, que entren en un *bucle*, en el cual siempre comprueben la ocupación del canal y emitan a la vez, tras esperar el tiempo AIFS, deberán realizar una segunda espera, durante un tiempo aleatorio que recibe el nombre de *Contention Window* (CW).

Este valor será obtenido, como un tiempo aleatorio entre un valor máximo y uno mínimo fijado en la red. De manera que dado su carácter de aleatoriedad, evitará en gran medida, que dos terminales accedan al medio en el mismo instante.
La variante de la norma 802.11e, basada en el algoritmo EDCA actúa sobre estos tiempos, AIFS, CW máximo y CW mínimo. En base a las cuatro categorías que contempla la norma, fija unos valores de tiempo AIFS menores, para las más prioritarias con respecto a las menos prioritarias. Así mismo los valores de CW máximo y CW mínimo, serán menores cuanto más prioritaria es la clase de tráfico. Todos estos valores, claramente serán menores que los valores adjudicados para el tráfico que no cumple con la 802.11e. Puesto que los tiempos que ha de esperar el tráfico más prioritario para volver a transmitir, será menor que el tráfico menos prioritario, estadísticamente se favorecerá la transmisión del tráfico más sensible y perteneciente a una clase de mayor prioridad que el menos sensible.

II.22.2.2. HCF Controlled Channel Access (HCCA)

Este sistema de QoS sobre redes WiFi, es más avanzado que el EDCA y permite un mejor control del tráfico emitido en la red. Sin embargo se considera opcional dentro de la certificación WiFi WMM. Su carácter no obligatorio, junto con la mayor complejidad de implementación, hace que pocos puntos de acceso y clientes WiFi lo implementen. Se puede entender el HCCA como una variación más elaborada del PCF. Un punto de

acceso que cumpla con HCCA, enviará una trama a cada uno de los clientes de forma secuencial, interrogándolos con el objeto de saber si disponen de tráfico para enviar, al igual que en el protocolo PCF.

La diferencia consiste en que ante esta trama, los clientes no responderán con un mensaje indicando que no disponen de tráfico para transmitir, o transmitiéndolo en caso contrarío, sino que informarán al punto de acceso si disponen de tráfico y que tipo de tráfico, es decir, cuanto tráfico, en cada una de las categorías previstas por la norma 802.11e, tienen esperando para ser enviado.
El punto de acceso, con el conocimiento del tipo de tráfico que tiene cada uno de los clientes, decidirá cual de ellos ha de transmitir. Así pues, será el punto de acceso quien indicará a los clientes elegidos que pueden transmitir y el intervalo que tienen para hacerlo. Con ello, al tener un director del tráfico con conocimiento y datos objetivos de decisión, se consigue una transmisión ordenada y que proporciona la calidad de servicio deseada.

Por su parte, los clientes deberán tener varias colas de espera, donde almacenarán los paquetes de cada una de las categorías por separado, para ser enviadas cuando el punto de acceso se lo indique. Así mismo deberán implementar un algoritmo de calidad, que permita priorizar el tráfico de las diversas categorías y enviarlo de la forma adecuada cuando tenga posesión del canal. Como puede verse, este método de control de la calidad de servicio, implica una mayor "inteligencia" en los dispositivos, lo que se traduce en: procesadores más potentes, más memoria, mejor y más elaborado software y todo ello implica un mayor coste, lo cual motiva que no suela ser implementado en los dispositivos WiFi de uso general.

II.22.3. Sistemas propietarios

Desde la aparición de la norma 802.11e y sobre todo desde la existencia de la certificación WiFi WMM, no existen sistemas propietarios WiFi que implementen redes *ad hoc* o del tipo infraestructura. Es lógico si tenemos en cuenta, que tanto el punto de

acceso como los clientes han de hablar el mismo protocolo y es fácil controlar el punto de acceso que se instala, pero en la mayoría de los casos, tener control sobre los clientes resultará imposible y estos serán de diversos fabricantes y por tanto incompatibles con sistemas propietarios.

El escenario cambia en los enlaces punto a punto, como la unión de edificios. En ese caso ambos extremos suelen implementarse con equipos del mismo fabricante, pues de otra forma lo más probable será que aparezcan problemas de incompatibilidades. Así mismo, este escenario permite muchas optimizaciones, pues no es necesario llevar un control de asociaciones de clientes, *roaming*, etc. De hecho, si la organización de la transmisión se realiza con un control duro, que podría ser similar al HCCA, podrían relajarse los protocolos de acceso al medio, con lo que se pueden obtener rendimientos mas elevados e implementar algoritmos de calidad de servicios propietarios más elaborados.

II.22.4. La necesidad de QoS en las redes WiFi

La funcionalidad de QoS en las redes WiFi, se está convirtiendo en un requisito clave, para soportar y/o admitir aplicaciones multimedia y la gestión del tráfico de red avanzada, en los diferentes segmentos de mercados de acceso residencial, empresarial y público.

II.22.4.1. Mercado residencial

En el mercado residencial, la demanda de aplicaciones multimediaWiFi está creciendo rápidamente en cuatro tendencias clave:

- Las redes domésticas WiFi, se están propagando rápidamente entre los hogares de banda ancha, ya sea una red doméstica centrada en la multimedia o una centrada en bases de datos, muy aparte de que WiFi ha surgido, como la tecnología inalámbrica para redes en el hogar.
- La penetración de la banda ancha residencial ha despegado.

- Nuevos servicios, contenidos digitales y nuevas aplicaciones (por ejemplo, VoIP, juegos, *streaming* de música) son cada vez más disponibles y la demanda de los consumidores es cada vez mayor.
- Una amplia gama de productos se están dirigiendo a la conectividad del entretenimiento digital y un mercado importante para el potencial de la conectividad WiFi están entrando rápidamente en el mercado.

II.22.4.2. Mercado empresarial

Las empresas necesitan urgentemente de QoS para ser capaces de soportar VoIP inalámbrica, la cual puede proporcionar ahorro de costos significativos y una conectividad inalámbrica de voz a través del campus, al levantar la infraestructura WiFi, evitando al mismo tiempo los costos tan elevados de los servicios celulares de voz. Otra aplicación que se beneficia de WMM, es la gestión de la prioridad del tráfico, que permite al administrador de TI asignar diferentes niveles de prioridad a diferentes usuarios. Por ejemplo, los administradores de red, tal vez deseen asignar una prioridad más baja a los visitantes que comparten la red, o para proporcionar más recursos a los empleados que trabajan en tareas críticas, o para aplicaciones como el video *streaming* o teleconferencia.

II.22.4.3. Mercado público

La gestión de la prioridad del tráfico, es también una clave para la capacidad de WiFi de acceso público. El uso de zonas WiFi está creciendo rápidamente con el número de *hotspots*. Están aumentando los usuarios acostumbrados a la VoIP y a las aplicaciones multimedia, tales como: *streaming* y juegos interactivos, que esperan poder utilizarlas también en zonas WiFi, poniendo una presión adicional sobre los recursos compartidos de la red. WMM puede ser utilizado, tanto para asegurar que esas aplicaciones específicas (ejem.: voz o juegos), tengan acceso a los recursos de la red requeridos o para que usuarios específicos reciban la prioridad en el acceso.

II.23. Tecnología Mesh [59], [60], [61], [62], [63], [64], [65], [66], [67]

II.23.1. La red Mesh: Una visión global

La topología *Mesh* supone un paso adelante, respecto de cualquier otra red inalámbrica aplicada a la videovigilancia. Fiabilidad y flexibilidad son las características principales de esta tecnología innovadora, cuya red dispone de nodos inteligentes, capaces de transmitir paquetes de datos recibidos de las otras unidades y decidir, en tiempo real, la mejor ruta en función de las condiciones de la red y el canal.

Las redes *Mesh* permiten instalar sistemas inalámbricos CCTV, tanto en presencia de obstáculos o fuentes de interferencia, como en cualquier otra situación en la que sea necesario prever la reinstalación de las videocámaras. La redundancia presente en esta arquitectura, permite colocar sistemas de videovigilancia con la misma fiabilidad que una red cableada, pero con una flexibilidad que sólo puede ofrecer un sistema inalámbrico.

II.23.2. Orígenes

Las redes *Mesh* tuvieron su origen en aplicaciones militares, con el fin de permitir a los soldados, tener comunicación confiable de banda ancha en cualquier lugar. De esta forma, la confiabilidad y robustez requerida en los entornos militares, se hereda a los ambientes civiles, donde las redes *Mesh* están encontrando un ámbito importante. Uno de los requisitos principales era, contar con comunicaciones de banda ancha sin tener que instalar grandes torres o antenas. Así, el equipo de radio de cada soldado, contribuía a la formación de una malla de unidades de radio, que automáticamente aumentaba su cobertura y robustez, conforme se unían nuevos usuarios a la misma.

II.23.3. Qué es WiFi Mesh

Una red WLAN tradicional, consta de uno o más puntos de acceso inalámbrico (Access Point), que se conectan mediante un cable UTP directamente a un switch/hub Ethernet hacia la red cableada. De esta misma manera, se podrían conectar más puntos de acceso para incrementar el área de cobertura de la red. Con las redes WiFi *Mesh,* es posible que estos puntos de acceso se puedan conectar y comunicar entre ellos de forma inalámbrica,

utilizando las mismas frecuencias del espectro disperso, ya sea en 2.4 GHz o en la banda de 5.8 GHz. Las redes WiFi *Mesh* son menos ambiciosas pero más reales y para operar sólo necesitan de clientes ordinarios IEEE 802.11. Comparado con otras tecnologías alternativas inalámbricas, WiFi es barata y ubicua, mientras que las terminales IEEE 802.16 (WiMax) son más aparatosas y cuestan más.

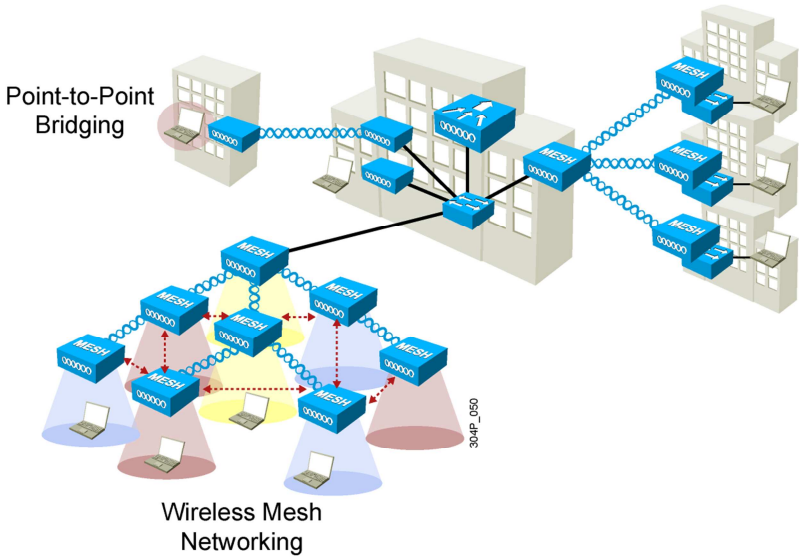

Figura II.17 Red Mesh

Las redes WiFi *Mesh* son simples, todos los *access points* comparten los mismos canales de frecuencia. Esto hace a los APs relativamente baratos y el único problema es que el canal es compartido, es decir, el ancho de banda de la red. Los APs actúan como *hubs,* así la malla funciona de manera similar a una red plana, construida completamente de hubs; es decir, todos los clientes contienden para acceder al mismo ancho de banda.
Una de las desventajas de un sistema de canal único, es que no se puede transmitir y recibir al mismo tiempo, introduciendo un considerable retardo para cada salto. A pesar de estas desventajas, los sistemas de canal único, siguen siendo populares debido a su bajo costo, sin embargo para lograr una mejor calidad y cobertura, se necesitarán sistemas de radio con canales duales o múltiples.

Los sistemas multiradio, utilizan un canal para enlaces hacia los clientes WiFi y el resto para enlaces en malla hacia otros APs. En la mayoría de las arquitecturas, los enlaces a

los clientes están basados en 802.11b/g, debido a que la banda de frecuencia de 2.4 GHz es la más utilizada por el hardware de los equipos WiFi. En cambio la red *Mesh* está basada en el estándar 802.11a, debido a que la banda de 5 GHz está menos congestionada, habiendo menos riesgo de interferencia entre los enlaces de la malla y los clientes. Sin embargo, el estándar 802.11 no soporta las mallas, así que cada fabricante necesita implementar su propia tecnología propietaria por encima del 802.11a. El estándar 802.11s, tiene la finalidad de reemplazar estas tecnologías propietarias, tanto para sistemas de un solo canal o de varios canales de radio.

II.23.4. Los beneficios

Las redes *Mesh* han ido cobrado importancia por las características que presentan, ya que ofrecen soluciones integrales, con redes de comunicación inalámbrica de banda ancha para la transmisión de voz, datos y video, permitiendo soluciones atractivas sin la necesidad de cables, lo que desemboca en movilidad del usuario. Es por esto, que para el diseño de un sistema que mitigue o perfeccione las comunicaciones en cualquier ambiente, es factible el uso de las redes *Mesh;* pues se asegura tener comunicaciones de: voz, datos y video móviles simultáneos. Sin embargo es importante evaluar sus capacidades y determinar de manera real los alcances que tiene. Las redes WiFi *Mesh* son útiles en lugares donde no existe cableado UTP, por ejemplo en oficinas temporales o edificios tales como bodegas o fábricas. Pero muchos de los fabricantes se están concentrando más bien en ambientes exteriores y en muchos lugares se ha incrementado el Internet público sobre redes WiFi, tales como aeropuertos o comercios. Quizá WiFi *Mesh,* sea un modesto competidor de otra tecnología más madura, conocida como WiMax. Un aspecto fundamental del funcionamiento de las redes *Mesh*, es que la comunicación entre un nodo y cualquier otro, puede ir más allá del rango de cobertura de cualquier nodo individual. Esto se logra haciendo un enrutamiento multisaltos, donde cualquier par de nodos que desean comunicarse, podrán utilizar para ello, otros nodos inalámbricos intermedios que se encuentren en el camino.

Esto es importante, si se compara con las redes tradicionales WiFi, donde los nodos deben de estar dentro del rango de cobertura de un AP y solamente se pueden comunicar con otros nodos mediante los APs; estos APs a su vez, necesitan de una red cableada para comunicarse entre sí. Con las redes *Mesh,* no es necesario tener AP, pues todos los nodos pueden comunicarse directamente con los vecinos, dentro de su rango de cobertura inalámbrica y con otros nodos distantes, mediante el enrutamiento multisalto ya mencionado.

Otro beneficio importante de las redes *Mesh*, es que presentan costos de operación más bajos que las redes WiFi tradicionales, ya que tienen capacidades de autoconfiguración y de reconfiguración. Esto es posible mediante sofisticados protocolos, que permiten el descubrimiento automático de rutas y el redescubrimiento de las mismas en caso de falla en algunos nodos. Dada esta capacidad de reconfiguración, las redes *Mesh* también resultan ser muy flexibles y robustas, pues la falla de uno o más nodos, no impide el funcionamiento de la red y no se presenta un punto crítico de falla (como sucedería por ejemplo si falla el AP en una red WiFi tradicional). Las características más relevantes de las redes inalámbricas *Mesh* son las siguientes:

- **Robustez:** La presencia de enlaces redundantes entre los usuarios, permite que la red se reconfigure automáticamente ante fallas.
- **Topología dinámica:** Se supone que las redes *Mesh* tienen la capacidad de reaccionar ante cambios de la topología de la red, por lo tanto la topología cambiante es una condición de diseño necesaria.
- **Ancho de banda limitado:** Como el proceso de comunicación exige transportar datos de otros usuarios y la cercanía de unos con otros precisa una coordinación en los tiempos de transmisión, las redes *Mesh* cuentan con enlaces, que usualmente permanecen en condiciones de congestión. Las primeras versiones de redes *Mesh* basadas en el estándar 802.11, son bastante ineficientes en el aprovechamiento del espectro.

- **Seguridad:** La información transmitida se encuentra expuesta a la amenaza de viajar a través de un medio compartido. El estándar define una subcapa de seguridad para proteger la información de los usuarios y evitar el acceso de usuarios no autorizados.
- **Canales de comunicación aleatorios:** A diferencia de las redes fijas, las redes inalámbricas cuentan con la incertidumbre propia de los canales de comunicación de radio. La característica cambiante de los mismos, hace bastante inciertas las condiciones de comunicación. El estándar define aspectos como la modulación y codificación adaptativas para hacer frente a este problema.
- **Carencia de modelos de dimensionamiento apropiados:** El modelo de capacidad de redes de datos, está orientado a determinar la capacidad del enlace, ante procesos de multiplexación de la información de los usuarios. El modelo de capacidad de las redes *Mesh* de múltiples saltos es un problema abierto. Las redes Mesh proveen, sin embargo, condiciones que permiten el acceso a usuarios en regiones apartadas.

II.23.5. Características técnicas

Las redes inalámbricas Mesh, o redes de malla inalámbricas, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología *ad hoc* y la topología infraestructura. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos, que a pesar de estar fuera del rango de cobertura de los puntos de acceso, están dentro del rango de cobertura de alguna tarjeta de red (TR), que directamente o indirectamente está dentro del rango de cobertura de un access point (AP).

Permiten que las tarjetas de red se comuniquen entre sí, independientemente del *access point.* Esto quiere decir que los dispositivos que actúan como tarjeta de red, pueden no mandar directamente sus paquetes al *access point,* sino que pueden pasárselos a otras tarjetas de red para que lleguen a su destino. Para que esto sea posible, es necesario el contar con un protocolo de enrutamiento, que permita transmitir la información hasta su destino con el mínimo número de saltos, o con un número que aun no siendo el mínimo, sea suficientemente bueno. Es resistente a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

La tecnología *Mesh* utiliza los estándares establecidos de una forma totalmente novedosa. El conjunto de nodos proporciona una zona de cobertura inalámbrica muy extensa. Los nodos son capaces de establecer comunicación entre ellos, en cuanto sus zonas de cobertura se sobreponen entre sí.

Por otro lado, si se sobreponen varias zonas de cobertura, aunque fallen uno o más nodos, la red se sustenta y sigue operando. El usuario probablemente ni se enterará de esto, ya que su equipo se conectará automáticamente (*roaming*) con el nodo más próximo operativo. Cuantos más puntos de acceso a Internet disponga, más fiable y rápida será la red.

La red está constantemente preocupada de saber, cuál es el mejor y más expedito camino para llevar la información hacia su destino, mediante la selección óptima de una trayectoria constituida, por uno o más saltos entre *access points*. Así, por ejemplo, si un usuario está enviando información hacia internet por una trayectoria y esta se ve obstruida por algún motivo, la red reenruta de manera inmediata y automática ese tráfico, por cualquiera de los caminos alternativos que existan en la red WiFi.

La tecnología de *Mesh* ofrece a los usuarios, la capacidad de estar en movimiento dentro de un área determinada de cobertura. Por ejemplo, dentro de una red inalámbrica *Mesh,* un usuario no perdería conectividad cuando se mueve de un *hotspot a* otro, puesto que los puntos de acceso en ambos hotspots, estarían comunicándose constantemente para ofrecer conectividad continua.

II.23.6. Ventajas y Desventajas de una red Inalambrica Mesh

II.23.6.1. Ventajas

Refiriéndonos más específicamente a una red 802.11, los puntos a favor de una red *Mesh* son numerosos:

- Hay un ahorro sustancial en materia de cableado, debido a que sólo se necesita un nodo conectado a una red (como el Internet) y el resto simplemente debe estar al alcance del anterior, para que puedan repetir la señal y aumentar la cobertura de la red.
- Fácil despliegue. Un nodo de una WMN, necesita únicamente mantenerse en el rango de cobertura de otro, un lugar en el cual ubicarlo (en una pared o un poste) y una fuente de energía. Esto hace a las WMN muy atractivas para soluciones inalámbricas Municipales.
- Gran autonomía, en el sentido de que pueden auto-curarse después de que un nodo o un enlace, haya tenido algún inconveniente.
- Instalación relativamente sencilla, para fabricantes que tienen soluciones *Mesh* específicas.
- Otra ventaja es, que gracias a que disponemos de varios nodos en una misma zona, las distancias a alcanzar no son tan grandes, por lo que se puede tener una disminución de las interferencias y un ahorro de energía, ya que no hace falta transmitir a tanta potencia.

II.23.6.2. Desventajas

Las redes *Mesh* todavía enfrentan algunos desafíos para una adopción más amplia y rápida. Uno de ellos se refiere a los indeseables efectos de las interferencias. Otro se refiere al *throughput* presentado por la red que todavía necesita ser adaptado. Por fin, el desafío mas relevante a ser destacado, se refiere a la falta de estandarización tecnológica, que dificulta sobremanera la inter-operabilidad entre equipamientos de diferentes proveedores. La cuestión de las interferencias se debe a la adopción de una frecuencia no licenciada para la operación. Así, las señales transmitidas quedan sujetas a interferencias provenientes de otras fuentes, que también operan en la misma banda, como por ejemplo: hotspots WiFi. Este punto fue detectado por algunos fabricantes de equipamientos, que desarrollan productos con características que permiten la autogestión de la radiofrecuencia.

II.23.7. Debilidades y Limitaciones de las Redes Inalámbricas Mesh

II.23.7.1. Rendimiento

El tema de la disminución del rendimiento (througput) existe en todas las redes multisalto. El rendimiento disminuye con el número de saltos de acuerdo a 1/n o 1/n2 o 1/n1/2, dependiendo del modelo ("n" es el número de saltos) que se utilice.

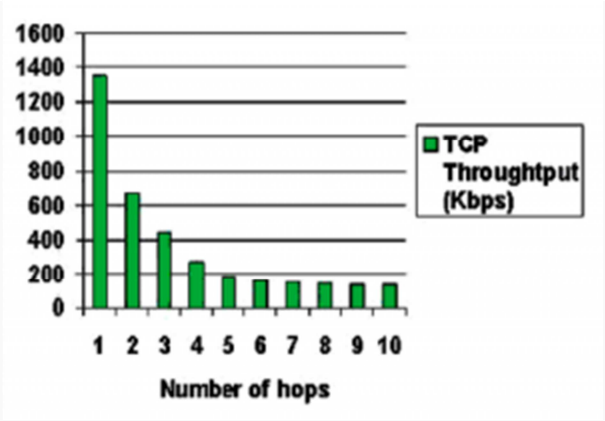

Figura II.18 Rendimiento del TCP para el MAC de 802.11 en función del número de saltos (Hops)

II.23.7.2. Escalabilidad

Todavía son limitadas las aplicaciones de *Mesh* en términos de número de nodos, pero algunas de las conocidas son las siguientes:

- Rooftop de MIT: 4050
- Berlín OLSR: cerca de 4000
- CUWin: cerca de 500
- Dharamsala: > 50

En las implementaciones comerciales a menudo no se comparte la experiencia (verdadera) abiertamente y por lo tanto son difíciles de evaluar.

II.23.7.3. Seguridad

Las redes *ad hoc* por definición, necesitan hablar con los clientes antes de autenticarlos, esto constituye un reto en la seguridad de Internet. Las redes *Mesh* son por diseño, muy

vulnerables a ataques de negación de servicio. *(Denial of service – DoS)*

.

II.23.8. Arquitectura de una Red Inalámbrica Mesh

Una red WMN puede estar diseñada de acuerdo a tres diferentes arquitecturas de red, basadas en topologías de red: WMNs planas, WMNs jerárquicas y WMNs hibridas.

- **WMNs Planas:** En una WMN plana, la red esta formada por los dispositivos del cliente que actúan como rebajadoras. Aquí, cada nodo está en el mismo nivel que el de sus pares. Los nodos inalámbricos del cliente, coordinan entre sí mismos para proporcionar el enrutamiento, la configuración de red, el aprovisionamiento del servicio y otros aprovisionamientos de uso.

  Esta arquitectura, es la más cercana a una red inalámbrica *ad hoc* y es el caso más simple entre las tres arquitecturas de WMN. La ventaja primaria de esta arquitectura es su simplicidad y sus desventajas incluyen la carencia del escalabilidad de la red y de los altos costos de recursos. Los problemas primarios a la hora de diseñar una WMN plana son: el esquema de dirección, el enrutamiento y el descubrimiento de esquemas de servicio. En una red plana, la dirección es una de los problemas que pueden convertirse en un embotellamiento contra la escalabilidad.

- **WMNs Jerárquicas:** En un WMN jerárquica, la red tiene grados múltiples o niveles jerárquicos, en los cuales los nodos del cliente de WMN forman o están en la parte más baja de la jerarquía. Estos nodos clientes, pueden comunicarse con la red troncal formada por *routers* de WMN. En la mayoría de los casos, los nodos de WMN, son los nodos dedicados que forman una red troncal de WMN. Esto significa que los nodos de la red troncal no originan o terminan los datos, en un tráfico determinado como los nodos del cliente de WMN. Su responsabilidad es el mismo de organizar y de mantener la red y proporcionar paquetes a los *routers* de WMN, algunos de los cuales, en la red troncal puede tener interfaces externas al Internet.

- **WMNs hibridas:** Éste es un caso especial de WMNs jerárquica, donde el WMN utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras

WMNs basadas en infraestructura tales como: redes celulares, redes de WiMAX, o redes basadas en los satélites. Ejemplos de tales WMNs híbridas, incluyen las redes celulares multihop, rendimiento de procesamiento de radio realzada en las redes locales del lazo y redes *ad hoc* de celulares unificadas. Puesto que el crecimiento de WMNs, depende grandemente de la manera como trabaja con otras soluciones inalámbricas existentes de una red, esta arquitectura llega a ser muy importante en el desarrollo de WMNs.

II.23.9. Criterios de diseño en redes inalámbricas Mesh multiradio (MR- WMNs)

Las principales ventajas de utilizar redes MR-WMNs, son el aumento de la capacidad, escalabilidad, fiabilidad, robustez y flexibilidad de implementación. A pesar de las ventajas de utilizar un sistema de multiradio para WMNs, existen muchos desafíos para el diseño de un sistema eficiente MR-WMNs. En esta sección se examinan las cuestiones a tener en cuenta para el diseño de una MRWMNs. Las principales cuestiones pueden clasificarse en: diseño de la arquitectura, diseño MAC, diseño de protocolos de enrutamiento y diseño de métricas, que se explican a continuación.

II.23.9.1 Criterios de diseño arquitectónico

La arquitectura de red, desempeña un papel importante para obtener un buen rendimiento de una red MR-WMNs. Cuando se diseña una red MR-WMN, la arquitectura seleccionada debe tomar en cuenta el tipo de aplicación y el escenario. Las principales opciones de arquitectura para ser consideradas son las siguientes: (a) basada en la topología, (b) basada en la tecnología y (c) basada en el nodo. Una MR-WMNs basada sobre la topología, se puede diseñar ya sea como topología plana o topología jerárquica**.** Hay que tomar en cuenta que las posibles soluciones en cuanto a arquitectura, es que las tecnologías utilizadas son homogéneas o heterogéneas. Aunque la forma más general para sistemas MRWMNs son tecnologías homogéneas, es decir utiliza un solo tipo de tecnología de radio, como la popular tecnología de conexión inalámbrica IEEE

802.11. Es posible desarrollar una red MR-WMNs con tecnologías heterogéneas que utilizan una variedad de tecnologías de comunicación.

Por último, la arquitectura basada en el nodo pueden clasificarse dentro de las siguientes: basado en el *host,* basado en la infraestructura, o redes híbridos MR-WMNs. En el caso de las basadas en *host* MR-WMNs, la red está formada por los nodos *host* y tiene una similar operación a la de una red *ad hoc* pero con limitada movilidad. Por otra parte la arquitectura de red MR-WMNs, basada en infraestructura, está formada por nodos situados en infraestructuras fijas o edificios. Por último una arquitectura de red híbrida MR-WMN, que opera tanto basada en infraestructura troncal y *host* inalámbricos en malla. Estos *hosts* se comunican a través de *backbone* inalámbricos en malla.

Esta topología de red troncal, se puede organizar bien como una topología plana o como una topología jerárquica. En algunos entornos de aplicación, los *hosts* son móviles y ellos también retransmiten tráfico en beneficio de otros *hosts* en la red. Un ejemplo de este tipo de red híbrida MRWMNs, es una red WMNs vehicular, que se comunica a través de una infraestructura inalámbrica Mesh. Por lo tanto, el diseño de un sistema MRWMNs, debe considerar el tipo de aplicación y el entorno de despliegue para la elección adecuada de una arquitectura.

II.23.9.2. Diseño para la capa MAC

La capa MAC para MR-WMNs se enfrenta a varios problemas, entre ellos tenemos la interferencia inter-canal 6, interferencia inter-radio 7, distribución del canal y el diseño de protocolos MAC. Por ejemplo para la interferencia inter-canal en IEEE 802.11b, aunque hay un total de 11 canales sin licencia en América del Norte (13 en Europa y 14 en Japón), sólo 3 de ellos (los canales 1, 6, y 11 en América del Norte) pueden ser utilizados simultáneamente en cualquier ubicación geográfica. Por lo tanto, la presencia de múltiples sistemas de radios en una misma zona se debe considerar la interferencia inter-canal, esta interferencia con el canal vecino, dará lugar a una degradación significativa del rendimiento.

La interferencia inter-radio se debe principalmente al diseño de los componentes de hardware y de la propia interfaz. La separación física de las interfaces pueden ayudar a evitar este problema en cierta medida, en algunos casos la separación puede ser difícil, especialmente en nodos móviles. Otra cuestión de importancia para MAC es el canal de distribución. Se trata de un proceso en que la asignación de canales sin interferencia daría lugar a un rendimiento alto y un buen acceso al medio. El canal de distribución debe considerar el número de canales disponibles y el número de interfaces disponibles.

Por último, lo más importante es el diseño de protocolos MAC. Esta disponibilidad de múltiples interfaces y múltiples canales que conducen a nuevos diseños para protocolos de acceso que deben beneficiar la presencia de múltiples radios. Algunos ejemplos de estos protocolos son: MCSMA, ICSMA, 2P-TDMA. Estos protocolos utilizan simultáneamente múltiples canales y también tratan de resolver la cuestión de acceso a los medios en MR-WMNs.

II.23.9.3. Diseño de protocolos de enrutamiento

El diseño de protocolos de enrutamiento depende del diseño de la arquitectura de la red WMNs y que en algunos casos, también depende de la aplicación de la red y del entorno de despliegue. El Diseño de protocolos de enrutamiento se puede clasificar en varias categorías: (a) la topología de enrutamiento, (b) enrutamiento en el *backbone* y (c) la información de mantenimiento de enrutamiento. Sobre la base de la topología de enrutamiento, los protocolos de enrutamiento se pueden diseñar, ya sea para un solo nivel o protocolos de enrutamiento jerárquico.

En el enrutamiento jerárquico, una jerarquía de enrutamiento se construye entre los nodos, de tal manera que la responsabilidad de enrutamiento se delega a los nodos de mayor nivel jerárquico, cuando el nivel de nodos de inferior jerarquía no puede establecer la ruta.

Por otra parte, en un sistema de enrutamiento de un solo nivel, este no tiene incorporadas las jerarquías y cada nodo tiene la misma responsabilidad para encontrar un camino para

el destino y participar en el proceso de enrutamiento. El camino elegido puede incluir cualquier nodo en la red, sin seguir ningún orden jerárquico. La segunda categoría de diseño se basa en el enrutamiento de rutas troncales y la topología de enrutamiento híbrido.

II.23.9.4. Diseño de métricas de enrutamiento

Una métrica de enrutamiento es una técnica utilizada por los *routers*. Es para aprender rutas y mantenerlas actualizadas, conforme cambia la red y su función principal es el intercambio de información de ruteo con otros *routers y* la información se encuentra en las tablas de ruteo. Las métricas incluyen ancho de banda, costo de la comunicación, retraso, número de saltos, costo de la ruta y confiabilidad. Contar los saltos es la más simple métrica de enrutamiento y es además de enrutamiento aditivo.

Debido a las características especiales de una red WMNs, la métrica de enrutamiento desempeña un papel crucial en el desempeño de un protocolo de enrutamiento y el diseño de métricas de enrutamiento debe tomar en cuenta varios factores, como: (a) la arquitectura de red, (b) el entorno de red, (c) la dimensión de la red, (d) las características básicas del protocolo de enrutamiento, con el fin de diseñar un eficiente protocolo de enrutamiento para WMNs.

II.23.9.5. Topología de control de la red

Topología de control se define, como la capacidad de manipular, tanto los parámetros de la red como la ubicación de los nodos, la movilidad de los nodos, la energía, las propiedades de la antena y las interfaces de red. La topología de control tiene la capacidad de modificar, ya sea una sola vez los parámetros durante la actividad de la red, en la fase de inicialización o como una actividad periódica durante el tiempo de funcionamiento de la red. El uso eficaz de la topología de control de la red, puede ayudar a mejorar la capacidad. Los objetivos de los mecanismos de topología de control son: la conectividad, la capacidad, fiabilidad, tolerancia a fallos y la cobertura de la red.

II.23.10. Soluciones multiradio para la capa enlace

La escalabilidad de la red, es el más importante problema que afecta en gran escala a una red WMNs. Las razones principales, detrás de la falta de escalabilidad en una red WMNs son las siguientes: (a) el carácter *half-duplex* de los radios WLAN, (b) las colisiones debido al problema del terminal oculto, (c) la pérdida de recursos debido a problemas del nodo expuesto y (d) las dificultades en el manejo de un sistema multicanal. Algunos de los problemas antes mencionados pueden ser resueltos por una MR-WMN. Existen varias soluciones de capa de enlace, tales como el protocolo de unificación multiradio (MUP) que se analizan a continuación.

II.23.10.1. Protocolo de unificación multiradio [MUP]

El MUP es una solución de capa de enlace, para proporcionar una capa virtual que controla múltiples interfaces de radio, a fin de optimizar el uso del espectro en una red MR-WMNs. Los principales objetivos de diseño del protocolo MUP son los siguientes: (a) reducir al mínimo las modificaciones de hardware, (b) evitar hacer cambios en los protocolos de capa superior.

El MUP proporciona una única interfaz virtual a las capas superiores, ocultando las múltiples interfaces físicas y canaliza mecanismos de selección para escoger un canal adecuado para la comunicación entre nodos. MUP es implementado en la capa enlace y por tanto las capas superiores no necesitan experimentar ningún cambio, para utilizar de forma eficiente múltiples interfaces de radio. El diagrama de arquitectura MUP se muestra en la siguiente figura.

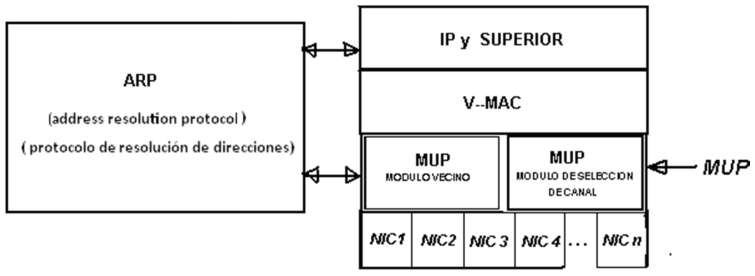

Figura II.19 Protocolo de unificación multiradio (MUP)

Una de las principales tareas que hace la capa MUP, es vigilar la calidad del canal entre un nodo y sus vecinos, de tal manera que el nodo puede elegir la mejor interfaz para comunicarse con un nodo vecino. Con el fin de virtualizar múltiples interfaces de radio con una dirección MAC diferente, MUP utiliza una dirección MAC virtual, que oculta eficazmente las múltiples direcciones físicas que tiene cada tarjeta de red inalámbrica. Esto hace que la capa física aparezca para las capas más altas como una única interfaz.

MUP emplea dos diferentes esquemas para la selección de interfaces de radio, estos esquemas son llamados MUP-Random y MUP-Channel-quality. De acuerdo con el esquema MUP-Random que es el esquema básico, un nodo al azar elige una interfaz para la transmisión de un paquete hacia un nodo destino. El esquema MUP-channel-quality está diseñado para mantener la información del estado del canal (conocida también como calidad métrica del canal), este esquema escoge entre algunos nodos y elige el mejor canal basado en mensajes de sondeo de información del estado del canal.

El uso de mensajes de sondeo permite a la capa MUP obtener información sobre el estado del canal. MUP consta de dos modulos: a) módulo vecino y b) módulo de selección de canal. El módulo vecino proporciona tablas y el estado de los canales de nodos vecinos. El módulo MUP de selección de canal, elige el canal más adecuado. Cada nodo elige y mantiene la información de calidad del canal para todas las interfaces, mediante el intercambio de mensajes de sondeo. El retardo del viaje de ida y vuelta experimentado por el mensaje de sondeo, es utilizado como canal de observación de la calidad de la métrica. Este retardo de viaje de ida y vuelta, incluye el retardo debido al protocolo MAC de contención, la carga de tráfico, las interferencias en el canal, las colisiones de paquetes y el retardo de procesamiento entre los nodos finales.

Con el fin de reducir el retardo, que en general podría ser muy alto en un nodo que tiene gran carga, MUP proporciona una alta prioridad para los paquetes de sondeo, ya sea colocando el paquete a la cabeza de los demás paquetes, mediante el uso de mecanismos de prioridad definidos en los protocolos MAC, tales como IEEE 802.11e. Las ventajas

de MUP son las siguientes: (a) puede trabajar con nodos que tengan una interfaz única o múltiples interfaces, (b) aísla a las capas superiores de conocer los protocolos que manejan múltiples interfaces de radio, y (c) mejora la eficiencia del espectro y el rendimiento del sistema.

Algunas de las desventajas son las siguientes: (a) la asignación de canales es ordinaria y por lo tanto MUP no podrá hacer uso de los mejores canales disponibles, (b) la exigencia de prioridad para los paquetes de sondeo, hace a MUP inutilizable en redes WMNs basadas en estándares IEEE 802.11a, IEEE 802.11b, IEEE802.11g, debido a que el protocolo MAC utilizado en estos estándares, no permite el uso adecuado de múltiples interfaces y (c) MUP decide cual canal utilizar en un nodo local y este canal a veces puede que no sea el más óptimo sobre los otros canales disponibles, esto afecta en la utilización adecuada de los recursos globales de la red.

Otra cuestión con MUP, es la asignación de canales para nuevos nodos que entran en funcionamiento en la red, para una red que tiene múltiples canales, se hace necesario el reinicio de todo el sistema, para determinar cuáles son los canales que se asignarán a las interfaces de los nuevos nodos con el fin que estos puedan comunicarse con el resto de la red.

II.23.11. Protocolos de control de acceso al medio para MR-WMNs

El diseño de protocolos MAC es importante en una red MR-WMNs, en comparación con redes WMNs de un solo radio, a causa de problemas adicionales que esta enfrenta. Aquí se presenta algunas de las recientes propuestas para protocolos MAC en redes MR-WMNs. Estos protocolos son los MCSMA y ICSMA.

II.23.11.1. Acceso múltiple por detección de portadora multicanal (MCSMA)

El protocolo MAC MCSMA es similar al sistema FDMA (Acceso múltiple por división de frecuencia). En este protocolo el ancho de banda disponible, se divide en anchos de banda más pequeños para tener n+1 canales, es decir, n canales de datos y un canal de

control. Esta división es independiente del número de nodos en el sistema. Un nodo que tiene paquetes para ser transmitidos selecciona un canal óptimo de datos para su transmisión.

Cuando un nodo está inactivo, es decir, no transmite paquetes de información, monitorea todos los n canales de datos y todos los canales por los cuales a recibido el TRSS (*total received signal strength* = total de intensidad de la señal recibida), el TRSS se estima por la suma de componentes individuales de señal de múltiples rutas, los canales que tienen un TRSS por debajo de ST (*sensing threshold* = sensibilidad del umbral) son marcados como canales inactivos. Cuando un canal está inactivo durante un determinado tiempo, se añadirá a la lista de canales libres. El mecanismo de transmisión de paquetes con el protocolo MCSMA es el siguiente.

Cuando un nodo potencial está en la capacidad de enviar y recibir paquetes de datos, comprueba en su lista de canales, si existe algún canal libre, el transmisor comprueba si el canal, por el cual transmitió con éxito el último paquete, está incluido en la lista de canales libres, se iniciará la transmisión por este canal. Si la lista de canales libres está vacía, espera a que un canal esté inactivo. Tras detectar un canal inactivo, el transmisor espera por un LIFS (*long interframe space* = gran espacio interframe), seguido por un acceso aleatorio *back-off*.
Después del período de *back-off* el transmisor comprueba nuevamente el canal, y si el canal está aún inactivo, se inicia la transmisión por ese canal.

En el caso de que el último canal utilizado para la transmisión, no esté presente en la lista de canales libres, el transmisor elige al azar un canal entre los canales inactivos, incluso en estos casos, el transmisor espera a que el canal siga inactivo durante el tiempo LIFS más el período de *back-off*. Si después de este tiempo el TRSS del canal supera al ST, entonces el proceso de *back-off* se cancela, cuando el TRSS del canal va por debajo de ST se inicia la transmisión. Si un canal está siendo ocupado para una transmisión

exitosa, se da prioridad a otro canal para poder entablar la transmisión, siempre y cuando n> N, donde n es el número de canales de datos y N es el número de nodos de la red.

II.23.11.2. Acceso múltiple por detección de portadora intercalada (ICSMA)

El ICSMA es un nuevo protocolo multicanal de acceso al medio. Está diseñado para superar el problema del terminal expuesto, que está presente en los sistemas de un solo canal, basados en detectar portadoras de los protocolos MAC, en una topología similar a la que se muestra en la figura.

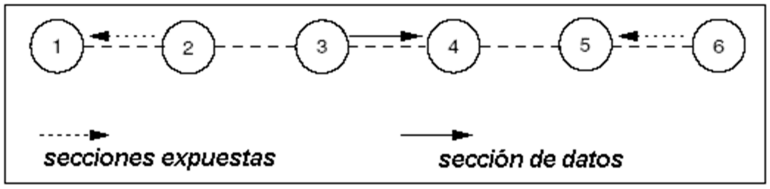

Figura II.20 Acceso múltiple por detección de portadora intercalado (ICSMA)

Cuando existe una transmisión en curso entre los nodos 3 y 4, los otros nodos en la red, es decir los nodos 2 y 6, no están autorizados a transmitir a los nodos 1 y 5 respectivamente. Esto se debe a dos razones: (a) ninguna transmisión simultánea del nodo 2 es posible, por su propio mecanismo de detección de portadora y (b) el reconocimiento de los paquetes recibidos por el nodo 3 también puede colisionar por la transmisión del nodo 2. Del mismo modo el nodo 6 es impedido para la transmisión, porque el reconocimiento de los paquetes originados por el nodo 5, podrían colisionar con la recepción de los paquetes de datos del nodo 4. Por lo tanto, los nodos 2 y 6 son designados como transmisor-receptor respectivamente. ICSMA es un sistema de dos canales de intercambio de paquetes. En comparación con el esquema CSMA/CA, el protocolo de proceso es intercalado entre los dos canales.

Por ejemplo en la Figura II.21, si un remitente RTS transmite en el canal 1 y si el receptor está dispuesto a aceptar la petición, envía la correspondiente CTS en el canal 2. Si el emisor recibe el paquete CTS, comienza la transmisión de paquetes de datos sobre el canal 1. En el receptor, si el dato es recibido con éxito, responde con paquetes ACK

en el canal 2. Figura 1.4 ilustra el funcionamiento intercalado de ICSMA cuando un nodo (S) envía un paquete RTS a un nodo receptor (R). En la Figura II.22 muestra la capacidad de transmisión simultánea entre los nodos A y B.

a. Paquetes intercalados para transmitir en ICSMA

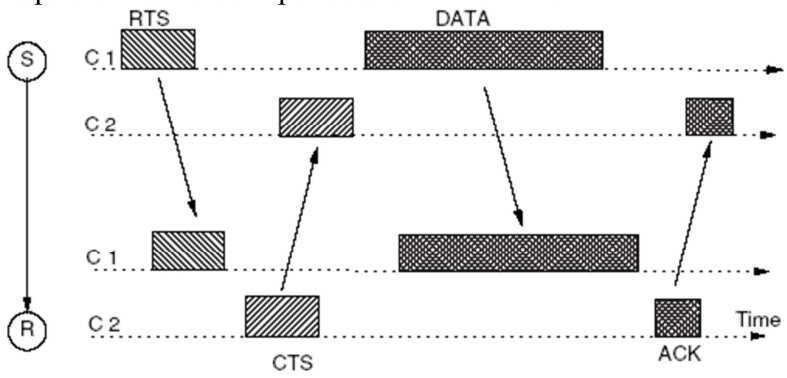

Figura II.21 Operación del protocolo ICSMA

b. Transmisión simultánea entre dos nodos

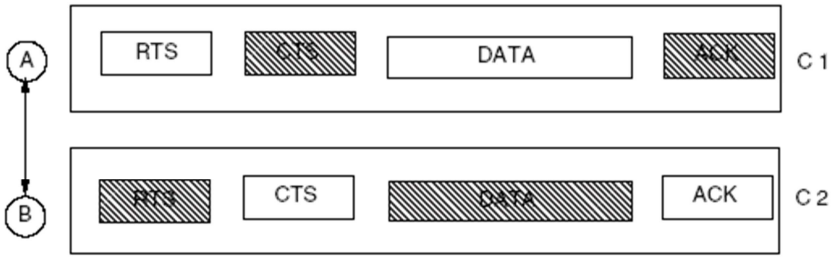

Figura II.22 Transmisión simultánea entre dos nodos

Este mecanismo intercalado de la portadora, aumenta el rendimiento alcanzado por los dos canales WMNs. El protocolo ICSMA utiliza una amplia red de distribución de vectores ENAV, para determinar si un canal en particular está libre para su transmisión. ENAV es una forma extendida de NAV utilizados para CSMA/CA.

II.23.12. Protocolos de enrutamiento multiradio para redes Mesh

Además del diseño de la arquitectura y del diseño del protocolo MAC, el rendimiento de una red WMNs y de una red MR-WMNs, se ven afectadas por el diseño del protocolo de

enrutamiento y las métricas de enrutamiento.

II.23.12.1. Métricas de enrutamiento para MR-WMNs

Al escoger la mejor métrica de enrutamiento en una red WMNs, se debe considerar ciertos factores que afectan el rendimiento de la red; y son los siguientes: (a) retardo inducido por la carga, (b) la asimetría de los enlaces inalámbricos y (c) la gran pérdida de enlace.

La nueva métrica (ETX) (transmisión esperada), se considera una buena métrica de enrutamiento que alcanza un alto rendimiento. Las métricas de enrutamiento
ETX están diseñadas para encontrar un camino basado en: (a) la distribución de los paquetes en cada uno de los enlaces, (b) la asimetría de los enlaces inalámbricos, y (c) número mínimo de saltos. Las ventajas de esta métrica son el ahorro de energía y la utilización eficiente del espectro.

La métrica de enrutamiento ETX ayuda a los protocolos de enrutamiento como DSR y DSDV, para encontrar un camino que proporcione un mejor rendimiento.
Esta métrica de enrutamiento ETX tiene una propiedad adicional; puede incorporarse dentro de otras métricas de enrutamiento, tradicionalmente basadas en el camino más corto y en la demanda. La ETX de un enlace es el número esperado de transmisiones con éxito, para ello es necesaria la transmisión de un paquete más sobre el enlace. La ETX de un extremo a extremo, se define como la suma de las ETX de cada uno de los enlaces de ese camino.

ETX de un enlace se calcula con la siguiente ecuación:

Donde:

$$ETX = \frac{1}{FDR * RDR} \qquad [Ec.\ 1.1]$$

FDR (forward delivery ratio) relación de entrega hacia delante.
RDR (reverse delivery ratio) relación de entrega inversa.

El FDR es el valor estimado de probabilidad de que un paquete de datos, sea recibido con éxito en el receptor durante un determinado enlace. Del mismo modo, el RDR es la estimación de probabilidad de que el paquete ACK, sea recibido con éxito en el transmisor. En la ecuación 1.1 el producto de FDR por
RDR, representa la probabilidad de una transmisión exitosa de un paquete de datos. El valor de ETX de un enlace, proporciona el porcentaje del número de intentos en la transmisión para enviar un paquete con éxito en un determinado enlace.

II.23.12.2. Calidad del enlace multiradio de enrutamiento de origen (MRLQSR)

MRLQSR es una extensión del protocolo DSR, está diseñado para trabajar con MR-WMNs. La principal contribución de MRLQSR, es el uso de una nueva métrica de enrutamiento llamado: ponderado acumulado de espera de tiempo de transmisión WCETT. El WCETT intenta evitar caminos más cortos de enrutamiento en una red MR-WMNs.

Los principales módulos en el protocolo MRLQSR son los siguientes: (a) un módulo vecino de descubrimiento, (b) módulo de asignación del enlace, (c) módulo para la propagación de la información y (d) módulo buscador de caminos. Los módulos vecinos de descubrimiento y módulo para la propagación de la información, son similares a las del protocolo DSR, mientras que los módulos asignación de enlaces y buscador de caminos, difieren de DSR. Mientras que DSR asigna igual peso a todos los enlaces, MRLQSR asigna enlaces amplios a caminos con un buen performance. El enlace asignado por el MRLQSR, es proporcional a la cantidad esperada de tiempo necesario para transmitir con éxito un paquete a través del enlace. Este tiempo de espera depende esencialmente, de la relación velocidad de transmisión de datos y de la tasa de pérdida de paquetes. Además, mientras que DSR utiliza un camino más corto de enrutamiento basado en saltos, MRLQSR usa WCETT como la métrica de enrutamiento.

La principal filosofía de diseño detrás de las métricas de enrutamiento WCETT, es obtener un enlace que nos indique el porcentaje de pérdida y el ancho de banda de un enlace, considerando la interferencia co-canal. La principal ventaja de MRLQSR, es el

rendimiento mejorado, en comparación con el rendimiento alcanzado por otras métricas de enrutamiento para multiradio como la ETX. Esta ventaja de rendimiento, se deriva del hecho de que MRLQSR considera el mejor camino, el retardo de extremo a extremo y el rendimiento para un conjunto de caminos. Esto lleva a la conclusión que WCETT en más eficiente que la métrica de enrutamiento ETX en alrededor del 80%. Uno de los inconvenientes más importantes es que MRLQSR no considera la interferencia de los canales vecinos.

Además, el uso de múltiples radios en un solo nodo pueden consumir más energía y la métrica de enrutamiento se encargará de utilizar, de mejor forma la energía cuando se utiliza en redes WMNs móviles. Esto puede hacer que la eficiencia MRLQSR, se reduzca cuando se utiliza en una red WMNs con movilidad limitada. Aunque WCETT no puede formar bucles de enrutamiento, cuando se utiliza con protocolos de enrutamiento bajo demanda como el DSR.

II.23.13. Redes Inalámbricas Mesh Multiradio y Multicanal

La relación costo-beneficio de las tecnologías de acceso inalámbrico, tales como IEEE 802.11, ha cambiado las comunicaciones y la informática de manera importante. Su éxito es debido a su despliegue en el hogar y en la pequeña empresa, donde se tiene cobertura limitada y sirve a sólo unos pocos usuarios a la vez. Actualmente existe un considerable interés en la ampliación de redes IEEE 802.11 a gran escala empresarial, para proporcionar una cobertura amplia y de banda ancha para el acceso a un número significativo de usuarios. Esto requiere de una proliferación de puntos de acceso (AP) en el área de cobertura deseada, bajo el estándar IEEE 802.11 con conjuntos de servicios básicos (BSSs). Para aumentar el alcance de la red (por ejemplo, entre un cliente y AP) se basa en reutilizar el espacio de frecuencias, asignándoles un conjunto de canales ortogonales de manera sistemática.

El valor de la señal de interferencia y ruido **SINR** (*signal to interference noise ratio*), en el extremo del BSS, junto con las propiedades inherentes del protocolo de la función de

coordinación distribuida (DCF), determinan esencialmente el rendimiento obtenido en el BSSs. La expansión de la red y el rendimiento global sobre el de área de cobertura, se pueden lograr mediante una combinación de enfoques, como el uso de antenas directivas; con esto lo más evidente que se logra es el aumento de la disponibilidad de ancho de banda en los sistemas (esto es equivalente a más canales ortogonales). Actualmente, sólo un número limitado de este tipo de canales ortogonales están disponibles: 3 en IEEE 802.11b (2,4 GHz) y 12 en IEEE 802.11a (5 GHz), está claro que el aumento de ancho de banda para la ampliación no es una opción viable.

Por consiguiente, para aumentar el rendimiento de la red, se requiere necesariamente de mejorar toda la pila de protocolos. Una opción prometedora para ampliar la capacidad de una red de acceso inalámbrico, es configurar la capa 2, que actualmente está previsto dentro del grupo de trabajo IEEE 802.11s. Esto implica una directa interconexión inalámbrica de un conjunto de nodos en malla para formar una red *multihop10*. Estos nodos forman parte de los APs que permiten el acceso directo de los clientes, así como "*routers* ", los cuales retransmiten solo paquetes, entre otros elementos de malla similar a una red *ad hoc.*

Para el diseño de redes de mayor cobertura, se deben modificar los mecanismos de topología, entre ellos el control de la energía y asignación de canales (CAs). Tradicionalmente las redes inalámbricas *multihop (*históricamente denominado redes de paquete de radio), están compuestos casi exclusivamente de un solo radio. Estas redes no están en condiciones de escala efectiva, para explotar los crecientes sistemas de ancho de banda disponible. En consecuencia, el uso de nodos de múltiples radios en una red *Mesh,* parece ser una de las vías más prometedoras para la expansión de la red. Varios radios aumentan en gran medida, el potencial para mejorar la selección del canal y la información de ruta, mientras la malla controla la interferencia y la topología de control permite controlar la potencia.

II.23.13.1. Arquitectura Mesh en 802.11

Se puede construir redes WMNs utilizando productos básicos de hardware IEEE 802.11. Sin embargo, antes de que esas redes pueden llegar a ser parte de los principales despliegues, se deben resolver algunas cuestiones como ser: seguridad, QoS y gestión de redes. Muchos de estos problemas son propios de cualquier red WMNs y no sólo de redes WMNs en base a IEEE 802.11.

La creciente disponibilidad de radios multimodo, integrados en las tarjetas 802.11a/b/g, de los clientes y dispositivos de infraestructura, permitirá implementar nuevas arquitecturas en malla. Los nodos en una malla para una red de acceso, consta de dos tipos como se muestran en la Figura II.23, un ligero predominio de puntos *Mesh* cuya única función es el enrutamiento de los paquetes de forma inalámbrica a los nodos vecinos y a otros subconjuntos de nodos *Mesh APs* que permiten la conexión directa con el cliente. Una pequeña fracción de estos nodos Mesh APs estarán conectados por el cable del *backbone* y sirven como puertas de entrada o de enlace para el tráfico de ingreso/salida.

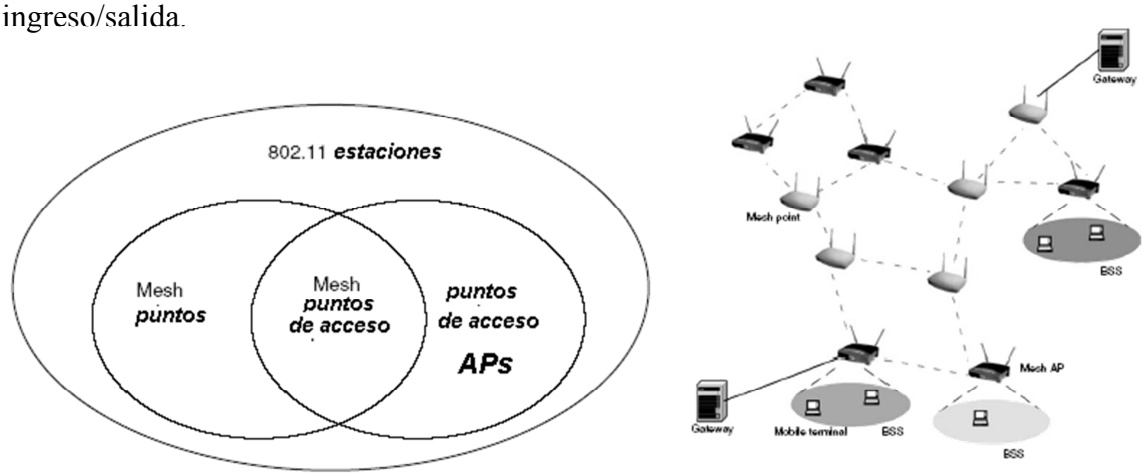

Figura II.23 Arquitectura Mesh en 802.11

II.23.13.2. Capacidad de expansión

El aumento del rendimiento de extremo a extremo, está relacionado con un aumento de los saltos, que a su vez depende del número de transmisiones simultáneas por canal. Esto se puede conseguir a través de muchos factores, como puede ser la topología de red y

varios atributos de los protocolos de pila de las capas 1, 2 y 3. Los atributos de la capa 1 incluyen el tipo de radio, requisitos del SINR en el receptor para la detección fiable y la propagación de la señal en medio ambiente.

Los atributos de la capa 2 incluyen control de acceso al medio MAC, atributos para controlar las interferencias y los atributos de la capa 3 incluyen la elección de las métricas de enrutamiento para determinar la mejor ruta. De este modo, la optimización global de la red requiere de un enfoque multidimensional, propuesta en el siguiente enfoque. En orden aparece la capa IP como una simple red de área local, una red *Mesh* puede aplicar su propia funcionalidad de enrutamiento y otros servicios a la capa "2.5", es decir, como una capa intermedia entre el estándar IEEE 802.11 MAC (o bajo MAC) y la capa IP. La figura ilustra esto para un nodo con dos radios.

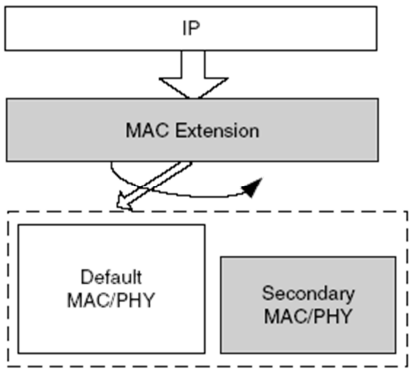

Figura II.24 Capacidad de expansión

II.23.13.2.1. Redes Mesh Multicanal de un solo radio

Cualquier ruta de extremo a extremo, en una red *multihop* deben utilizar todos los canales ortogonales disponibles. Una manera de mejorar el rendimiento de la red es maximizar la reutilización espacial, es decir, maximiza el número de transmisiónes simultáneas en el área de la red. Desafortunadamente existe una limitación en los dispositivos inalámbricos de un solo radio y es que operarán solamente en modo *half-duplex* y por lo tanto no puede transmitir y recibir simultáneamente, incluso, si múltiples canales están disponibles. Un posible enfoque *multihop,* es la formación de rutas para

todos los nodos que utilizan el mismo canal, aunque varios canales esten disponibles, sin embargo, evita el inconveniente de los grandes retardos de extremo a extremo, cuando los nodos adyacentes utilizan diferentes canales de comunicación.

Esta última requiere el escaneo de canales para realizar la conmutación y una radio activa tal, que dos nodos adyacentes comparten un mismo canal, lo que retarda la conmutación por nodo. Por ejemplo, el retardo de conmutación varía para el hardware en IEEE 802.11, desde unos pocos milisegundos a unos cientos de microsegundos. Esta frecuencia de conmutación de canales puede considerarse como una vía eficaz, debido a que el retardo de conmutación se manifiesta como un salto virtual a lo largo de la ruta.

De ahí que, aprovechando los múltiples canales ortogonales, claramente se mejora el rendimiento global con respecto a la hipótesis de un solo canal, pero a costa de aumentar el retardo de extremo a extremo. Por todas estas razones las red *Mesh* multiradio introducen varios y nuevos grados de libertad con respecto a la limitación de dispositivos inalámbricos de un solo radio, se espera que los dispositivos multiradio sean un componente clave en lograr escalabilidad y adaptabilidad (como un software definido para las múltiples radios) para las futuras redes inalámbricas.

II.23.13.2.2. Redes Mesh Multiradio

Los nodos con múltiples radios son efectivamente *full dúplex*, es decir, que pueden recibir en el canal C1 en una interfaz, mientras simultáneamente se transmite en el canal C2 en otra interfaz, con lo que se duplica el rendimiento en el nodo. La asignación de canales tiene una gran influencia en el rendimiento de extremo a extremo, al igual que la elección de métricas de enrutamiento para la formación de ruta. En resumen con buen diseño de las capas 1, 2, 3, aumenta el rendimiento de redes *Mesh* multiradio así como su tamaño.

II.23.13.3. Criterios para el uso de radios

Empezamos con un exámen de las posibles políticas de uso de radio, que determinan

cual radio en un nodo se utiliza para transmitir a un nodo en particular y cuando se obliga a la radio de un canal en particular. La aproximación más simple, para vincular los canales a las interfaces, es utilizar una vinculación estática. En este enfoque, cada interfaz está asignado a un canal, cuando el sistema se inicia y se mantiene permanentemente sintonizado a ese canal. En las redes modernas se utiliza una conmutación que tiene la tarea de asignación de canales para las interfaces en cada nodo.

La ventaja fundamental de utilizar vinculación estática, es que no requiere ningún cambio en el actual estándar IEEE 802.11. Sistemas más complejos, exigen un cierto nivel de coordinación entre los nodos, generalmente a través de una modificación del protocolo MAC. En redes MRMC (Multiradio Multicanal) el radio a usar para comunicarse con un nodo vecino, pasa a ser interesante en el caso que, cuando dos nodos vecinos tienen más de un canal en común, pueden comunicarse a través de más de una interfaz.

El protocolo multiradio de unificación MUP (*multiradio unification protocol*), combina múltiples interfaces disponibles, en una única interfaz lógica que se ha visto por la capa superior. EL MUP transmite datos a través de sólo uno de los interfaces disponibles, además selecciona la interfaz con el más bajo tiempo de ida, medida a través de un paquete de reconocimiento. Se muestra que en los casos donde la reordenación de los paquetes causa una importante pérdida de rendimiento, MUP puede mantener un alto rendimiento.

Enfoques híbridos (o mixtos), donde una interfaz se sintoniza a un canal fijo, mientras que la otra interfaz está cambiando dinámicamente a otros canales. Uno de ellos se describe que tiene un interfaz fijo, en cada nodo sintonizado a cualquiera de los canales disponibles y la elección del canal se comunica a los vecinos con un protocolo de capa superior. Cuando un nodo desea enviar un paquete a su vecino, cambia una de sus interfaces dinámicas para el canal fijo de los vecinos y transmite el paquete. De este

modo, el canal fijo para cada nodo representa el canal deseado para la recepción en ese nodo. Esta política se ilustra en la figura 1.7 para el caso de tres interfaces por nodo.

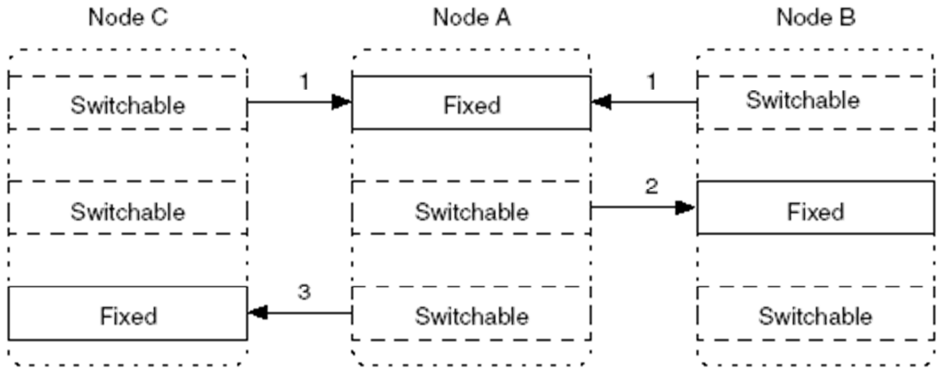

Figura II.25 Transmisión entre nodos

II.23.13.4. Asignación de canales y enrutamiento

En una topología típica, algunos de los nodos *Mes*h sirven como puertas de enlace y el tráfico, desde o hacia estos portales, pueden ser mucho más elevado que en otros lugares en la red. La carga de tráfico en cada enlace, se ve afectada por la elección de los protocolos de enrutamiento, así como por las métricas de enrutamiento. En una red WMNs, cuando un flujo se dirige por un determinado enlace, no sólo reduce la capacidad disponible de ese enlace, sino también la capacidad disponible en otros canales.

Esto se debe a que todos los enlaces dentro del canal, comparten el mismo ancho de banda total para sus transmisiones. La discusión anterior pone en manifiesto que existe una estrecha relación entre CAs y el enrutamiento en redes Mesh, con el fin de maximizar el rendimiento y los dos problemas deben ser tratados conjuntamente. Sin embargo, en la práctica el problema común es generalmente difícil de resolver óptimamente. Un enfoque para este problema común, es resolver la asignación de canales y los problemas de enrutamiento y actuar sobre las dos fases para mejorar el rendimiento global.

II.23.13.4.1. Asignación básica de canal

El problema básico de CAs se puede plantear en términos de asignación de canales, garantizando al mismo tiempo, que dos nodos vecinos tengan por lo menos un canal común (lo que asegura que los nodos vecinos puedan comunicarse). Un método de asignación aleatorio de canales para radios, puede que no sea factible. Consideremos, por ejemplo, una red en la que todos los nodos tienen dos radios y asignamos uno de los cuatro canales a cada una al azar. Si algún nodo está asignado a los canales 1 y 2 y a su vecino se le asigna los canales 3 y 4, esto lleva a que los dos nodos no tengan un canal en común y la sesión no es factible. El objetivo de varios algoritmos CAs, es la posibilidad de elegir un canal que mejor optimice el rendimiento. A continuación presentamos uno de estos algoritmos.

II.23.13.4.2. Métricas de enrutamiento

La métrica más simple de enrutamiento cuenta los saltos (el camino más corto), y ha sido ampliamente utilizado en los actuales protocolos de enrutamiento *Ad Hoc*, sin embargo estos protocolos funcionan mal en las redes de malla. Una perfeccionada métrica es la ETX (contar con la expectativa de transmisión). La métrica ETX asigna un peso a cada uno de los enlaces que correspondan, con el número esperado de transmisiónes requeridas por el 802.11 MAC, para transmitir con éxito un paquete sobre el enlace. Estas ETX, asignan un peso superior a los enlaces que están sujetos a una alta pérdida de paquetes. Esta es una mejora con respecto al enfoque de contar saltos, sin embargo, no cuenta el hecho de que los diferentes enlaces pueden usar diferentes anchos de banda, o la reutilización del mismo canal a lo largo de un camino, lo que reduce la capacidad disponible. La métrica ETT (expectativa de tiempo de transmisión).

Aborda el problema de múltiplexación de ETX, por el tiempo que necesita para cada transmisión.

II.23.14. Redes Mesh basadas en IEEE 802.11

IEEE 802.11 se ha convertido en el estándar de facto para: el hogar, la empresa y para el despliegue de redes de área local inalámbricas (WLANs). La mayoría de estos

despliegues operarán en el modo de infraestructura, donde un conjunto de puntos de acceso (APs), sirven de centros de comunicación para estaciones móviles y proporcionan puntos de acceso a Internet. El papel actual de IEEE 802.11, se limita a los clientes móviles que se comunican a través de APs. Las economías de escala hacen que IEEE 802.11 sea una alternativa deseable, incluso para interconectar estos APs en forma de una malla de red inalámbrica (WMN), como se muestra en la siguiente Figura.

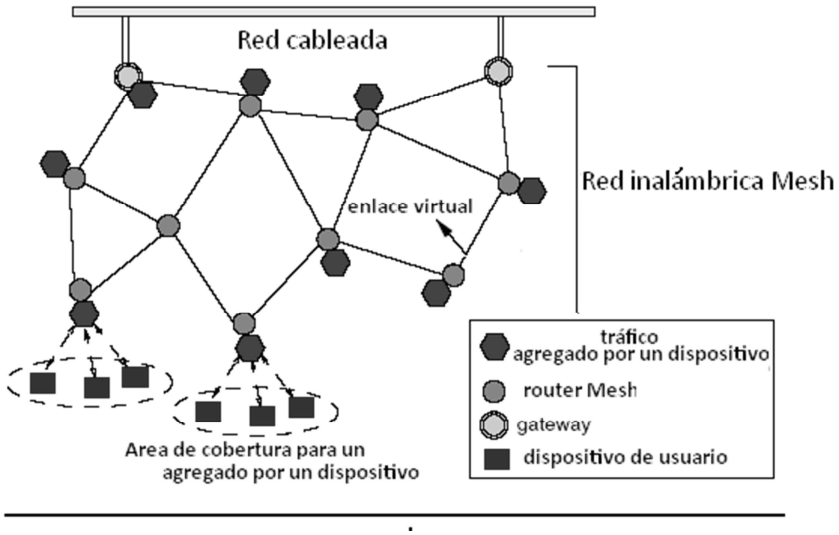

Figura II.26 Redes Mesh basadas en IEEE 802.11

Para satisfacer aplicaciones, IEEE 802.11 soporta dos modos de funcionamiento: el modo *ad hoc,* que con un solo salto en la red, todos los nodos *ad hoc* se comunican entre sí directamente, sin la utilización de un AP. EL segundo modo es el sistema de distribución inalámbrica (WDS), modalidad para la formación de transmisión punto a punto, donde cada AP no sólo actúa como una estación base, sino también como un nodo retransmisor inalámbrico.

Sin embargo, una red IEEE 802.11 puede utilizarse para formar una eficaz red WMNs. El rendimiento, la seguridad y la gestión son cuestiones que deben ser abordadas. Desde el primer punto de vista, el rendimiento bajo de extremo a extremo, es un problema común en redes WMNs basados IEEE802.11.

II.23.14.1. Problemas de rendimiento y sus causas

II.23.14.1.1. Capacidad limitada

A pesar de los muchos avances de la tecnología para la capa física (inalámbrica), la limitada capacidad sigue siendo una cuestión apremiante, incluso para redes WLAN de un solo salto. La publicidad de 54 Mbps de ancho de banda, para el hardware IEEE 802.11a/g, es el pico de velocidad de transmisión de datos.

Además, la máxima velocidad de transmisión en la capa enlace, decrece rápidamente al aumentar la distancia entre el transmisor y el receptor.

II.23.14.1.2. La interferencia Intraflujo e Interflujo

La cuestión del ancho de banda es aún más grave para redes WMNs, donde con el fin de mantener la red conectada a todos los nodos, ésta opera sobre el mismo canal de radio. Esto resulta en una interferencia sustancial de las transmisiones, entre nodos adyacentes en la misma ruta, así como en las rutas adyacentes la reducción de la capacidad de extremo a extremo de la red. La Figura II.27 representa un ejemplo de tal interferencia.

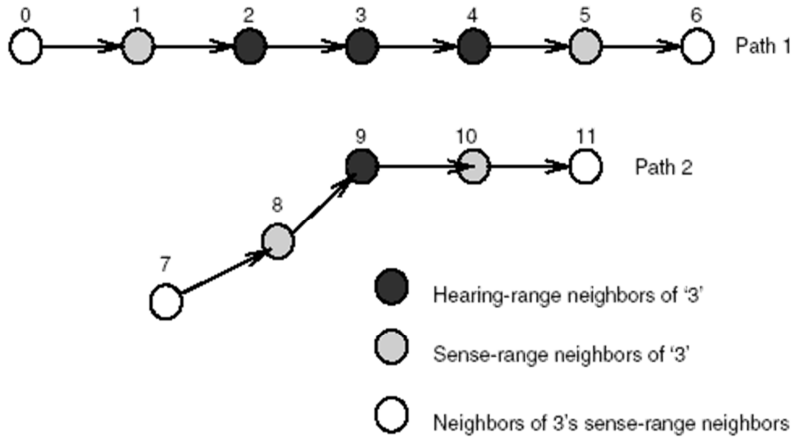

Figura II.27 La interferencia Intraflujo e Interflujo

II.23.14.1.3. Selección efectiva de ruta

La más simple métrica de enrutamiento para redes WMNs, es la métrica de contar los saltos, sin embargo, el uso de esta métrica de contar los saltos, conduce a una selección

no fiable de ruta. En primer lugar, contar los pequeños saltos se traduce en más tiempo y por tanto tendencia a más errores de salto individual. En segundo lugar, esta métrica no hace nada para equilibrar la carga de tráfico a través de la red. Esto reduce la capacidad efectiva de la red WMNs.

II.23.14.1.4. Control del overhead en TCP

El problema de la limitada capacidad se agrava, por el protocolo de control de transmisión (TCP), que no utiliza eficazmente el ancho de banda disponible. Primero, dada las características del TCP, obliga a enviar un paquete de reconocimiento con cualquier clase de paquete y estos paquetes consumen ancho de banda considerable (hasta el 20%), debido al alto y fijo *overhead* por paquete en redes inalámbricas IEEE 802.11. En segundo lugar, cuando un paquete se pierde entre los saltos, la estrategia del TCP de extremo a extremo, es la retransmisión del paquete por todo el camino nuevamente y esto conduce a un desperdicio del ancho de banda.

II.23.14.1.5. Ineficaz control de congestión

La congestión en el TCP, se basa en eliminar paquetes perdidos para detectar la congestión de la red. En las redes inalámbricas, sin embargo, los paquetes también se eliminan debido a errores. TCP no distingue entre estos errores poco frecuentes y los paquetes que producen la verdadera congestión. Según la condiciones del canal este puede dar lugar a una importante caída de rendimiento de la red.

II.23.14.1.6. El problema del terminal oculto

Es bien conocido que la capa MAC IEEE 802.11, exhibe el problema del nodo oculto, que causa que un enlace inalámbrico de transmisión, sea rechazado por otro enlace de utilidad para la transmisión. Mientras los mensajes RTS/CTS en el protocolo MAC 802.11, efectivamente detienen un nodo oculto que interfiere con una comunicación permanente en curso, no pueden impedir que el nodo oculto, inicie secuencias de mensajes RTS/CTS en tiempos inoportunos y se sufra largos tiempos de retardo, debido a la ejecución del algoritmo de *back-off*. TCP agrava este problema de flujo, porque el

remitente TCP promueve el algoritmo de *back-off*, cuando sus paquetes tardan mucho tiempo en llegar a través de los enlaces inhibidos. Como resultado, un flujo TCP atraviesa por un enlace y puede ser totalmente suprimido en el peor de los casos.

I.23.14.1.7. El problema de compartir el canal

Los protocolos de transporte existentes, hacen el mejor intento de asignar un canal de radio con un ancho de banda específico, entre los flujos de un solo nodo, en lugar de hacerlo entre todos los flujos, de todos los nodos que comparten el canal de radio.

Como resultado, un flujo emana de un nodo con menos densidad y con un ancho de banda de canal grande. La equidad del TCP depende en gran medida, del tiempo de ida y vuelta (RTT) de los flujos involucrados. Cuando dos flujos multi salto TCP comparten el mismo enlace inalámbrico, los flujos que atraviesa un número de saltos, tiende a adquirir más ancho de banda. Si bien esto es cierto, incluso para las operaciones de TCP en la internet por cable, el problema es mucho más frecuente en una red WMNs, porque en una red WMNs la mayor parte del tráfico se dirige hacia y desde los nodos *gateway* (nodos de puertas de enlace), que conectan una red WMNs al Internet por cable.

II.23.14.2. Alto rendimiento de enrutamiento

El enrutamiento gobierna y regula el flujo de paquetes a través de la red WMNs. Mientras más cortas sean las rutas de enrutamiento, se reduce al mínimo la cantidad de ancho de banda utilizada en la red, para transferir los paquetes y no considera factores importantes, tales como errores de enlace (enlaces críticos). La inteligente selección de las rutas en base a estos factores, pueden no sólo mejorar la calidad de la ruta elegida, para el actual flujo de paquetes, sino también, permitir la admisión de paquetes con más carga en la red. Existen diferentes técnicas de enrutamiento, que están todavía en estudio como ser:

- Enrutamiento vigilante de la calidad del enlace
- Enrutamiento vigilante de la interferencia
- Enrutamiento multicamino

- Enrutamiento vigente de la diversidad
- Enrutamiento oportuno

II.23.14.3. Redes Mesh multicanal

El estándar IEEE 802.11b/g y el estándar IEEE 802.11a, proporcionan 3 y 11 canales, respectivamente, que podrían ser utilizados simultáneamente con un nodo adyacente. La posibilidad de utilizar múltiples canales, aumenta sustancialmente la eficacia del ancho de banda disponible, para los nodos de la red inalámbrica. Sin embargo, una arquitectura convencional WMNs, equipa cada nodo con una sola interfaz, que siempre está sintonizada a un canal único con el fin de preservar la conectividad. Para utilizar múltiples canales dentro de la misma red, cada nodo necesita tener capacidad de conmutación de canal o estas necesitan múltiples interfaces, cada uno sintonizado para operar en un canal diferente. La conmutación de canal requiere, de una eficaz sincronización entre los nodos, en el momento en que cualquier nodo transmite o recibe en un canal en particular. Un posible esquema es, tener a todos los nodos de conmutación entre todos los canales disponibles en algún orden predeterminado. Aquí una interfaz cambia entre los canales disponibles, en diferentes *slots* de tiempo de forma aleatoria. Los nodos que deseen comunicarse, esperan una ranura de tiempo donde sus interfaces están en el mismo canal.

Estas secuencias no son fijas y pueden alterarse. La ventaja de este sistema es, que el tráfico de carga es equilibrado en todos los canales disponibles en general y logra la reducción de interferencias. Sin embargo, dicha sincronización es difícil de conseguir sin modificar la capa MAC 802.11, por lo tanto, utilizar *routers* WMNs multiradio, es un enfoque más prometedor para formar redes WMNs multicanal, basadas en IEEE 802.11.

La asignación de canales para interfaces de radio, juega un papel importante en el aprovechamiento de la capacidad de ancho de banda de esta arquitectura multiradio.

Por ejemplo, una idéntica asignación de canal para todos los nodos, limita sustancialmente el rendimiento que es posible alcanzar para arquitecturas de un solo radio. El objetivo de direccionar la asignación del canal, es reducir las interferencias

mediante la utilización de tantos canales como sea posible, manteniendo al mismo tiempo la conexión entre nodos. En esta sección se discuten, las diferentes técnicas propuestas para llevar a cabo la asignación inteligente de canal.

II.23.14.3.1. Asignación del canal basado en la topología

La asignación del canal, puede hacerse exclusivamente sobre la base de la topología de la red, con el objetivo de reducir al mínimo la interferencia en el enlace. El problema es computacionalmente difícil de conseguir, por lo que las soluciones propuestas son aproximadas. Una de las soluciones se revisa a continuación: el algoritmo denominado "conexión de baja interferencia de asignación de canal" (ClICA), revisa todos los nodos en el orden de calidad del canal y los nodos de menor calidad son visitados primero. Al visitar un nodo, los canales se eligen y se escoge el nodo local con el canal óptimo, porque el objetivo es reducir al mínimo la interferencia que se ejerce entre enlaces.

Existen otras soluciones para asignación de canal en redes *Mesh* basadas en IEEE 802.11.

- Asignación de canales mediante vigilancia de tráfico
- Asignación dinámica de canal

II.23.14.3.2. Interferencia Inter-canal

En experimentos que se han realizado con hardware 802.11, se analiza la interferencia entre dos tarjetas en la misma máquina. El grado de interferencia depende de las posiciones relativas de las tarjetas, por ejemplo: la colocación de tarjetas en la parte superior derecha de cada uno, lleva al máximo de la interferencia y sólo alcanza un máximo del 20% de ganancia. Con la pérdida del rendimiento debido a la interferencia intercanal, se encontró independencia de bandas, es decir, la degradación fue casi la misma cuando el canal 1 y 6 se utilizaron en comparación del caso, cuando el canal 1 y 11 fueron utilizados.

Se sospecha que esta interferencia surge debido a los filtros imperfectos presentes en las tarjetas. Este resultado tiene implicaciones por la colocación de varias tarjetas en la misma máquina y es necesario tener en cuenta las fugas electromagnéticas de dichas tarjetas. Debe encontrarse una posición adecuada para cada tarjeta y así reducir al mínimo la interferencia entre tarjetas. Una posible forma de lograrlo es, usando tarjetas USB con antenas externas, en vez de tarjetas PCI/PCMCIA.

II.23.14.4. Equidad de flujo

Un gran reto en redes *Mesh* IEEE 802.11, es asignar eficientemente el ancho de banda entre varios flujos en competencia. Como ya se discutió la capa MAC en IEEE 802.11 no distribuye equitativamente los flujos. A continuación se analiza uno de los criterios para la asignación adecuada de flujos.

II.23.14.4.1. Tasa implícita basada en el control de la congestión

WTCP es una modificación basada en el TCP, utiliza una tasa basada en el control de congestión, mide la relación del espaciamiento entre los paquetes del receptor y el transmisor, para determinar si aumentar o disminuir la tasa de transmisión. Si existe un cuello de botella a lo largo de la ruta, este es reflejado por el retardo entre paquetes en el receptor. Si la velocidad de transmisión de envío es inferior al ancho de banda disponible, los paquetes recibidos mantienen un costante espaciamiento.

En caso contrario, los paquetes de prueba que se utilizan para determinar el estado del enlace, podrían acumularse uno detrás de otro, lo que aumentaría el espaciamiento entre paquetes, por lo tanto el rendimiento del enlace bajaría. Este método asume que, todos los flujos en la red son atendidos en estricto orden de llegada, cuando se presenta un cuello de botella, para un enlace determinado. Esta hipótesis no se sostiene en redes WMNs basadas en el estándar IEEE 802.11, ya que la transmisión de paquetes en enlaces inalámbricos, tiende a ser a través de ráfagas. El tráfico de ráfagas que llegan al cuello de botella de un enlace, llegan sin espaciamiento entre paquetes.

II.23.15. Uso de las capas del modelo OSI en redes Mesh

II.23.15.1. Capa Física

A través del tiempo se han hecho comprobaciones, acerca de las técnicas avanzadas que se usan en esta capa y que están disponibles para las redes inalámbricas *Mesh y* se llega a la conclusión de que, debido a la gran densidad de nodos que poseen estas redes y al espectro limitado, es indispensable optimizar el uso de los canales, minimizando las interferencias.

Estos mecanismos son la selección dinámica de frecuencia (DFS) y el control de potencia (TPC). Con el fin de aumentar la capacidad y mitigar la interferencia entre canales, se han creado sistemas multi-antenas, como es el caso de: las antenas pequeñas y los sistemas MIMO, que hacen uso de esta tecnología, con el fin de conseguir capacidades superiores a los 108 Mbps en el enlace inalámbrico. Por otro lado existen otras tecnologías de radio que usan técnicas como ser: el acceso múltiple de la frecuencia ortogonal (OFDM) y la Banda ultra-ancha (UWB).

II.23.15.2. Capa MAC

Existen grandes diferencias, entre la capa de acceso al medio en una WMNs y las contrapartes clásicas de las redes inalámbricas. Las redes clásicas poseen serias limitaciones en los multisaltos, debido a los problemas del nodo oculto y del nodo expuesto. Existen mecanismos de acceso al medio, que son muy útiles para las redes *Mesh* como es el caso de: TDMA (Time Division Multiple Access) y CDMA (Code Division Multiple Access), los cuales pueden disminuir los efectos de las interferencias, ya que dos nodos pueden ocupar simultáneamente el mismo canal, empleando códigos diferentes.

Protocolos convencionales. La principal responsabilidad de los protocolos de la capa MAC, es asegurar el compartimiento de recursos. Hay dos grandes categorías de los esquemas MAC como: los protocolos basados en contención y los protocolos basados en libres colisiones de los canales. Los protocolos basados en contención, asumen que no

hay entidad central que asigne los canales en la red. Para transmitir, cada nodo debe contener su propio medio.

Las colisiones resultan cuando, más de un nodo trata de transmitir al mismo tiempo. Como es bien sabido, los protocolos basados en contención, incluyen Aloha, CSMA y CSMA/CA. En contraste, los protocolos de libre colisión, asigna canales dedicados a cada nodo que desea comunicarse. Los protocolos de libre colisión, pueden eliminar colisiones con eficacia, liberando asi los canales de alto tráfico. Ejemplos de estos protocolos son: el TDMA, CDMA y FDMA.

II.23.15.3. Capa de Red

A pesar de la disponibilidad de muchos protocolos de enrutamiento para las redes *ad hoc*, el diseño de los protocolos de enrutamiento para WMNs, sigue siendo un área activa de la investigación. En realidad el protocolo óptimo de enrutamiento para WMNs debe tener estas características:

• ***Métrica de funcionamiento múltiple****:* Consiste en escoger la trayectoria adecuada para el envío de paquetes.
• ***Escalabilidad:*** Se requiere el uso de un protocolo que perdure mucho tiempo en funcionamiento y que sea útil para las nuevas tecnologías, puesto que las WMNs aún no se han explorado por completo.
• ***Robustez:*** Consiste en evitar la interrupción del servicio, WMNs debe ser robusto para ligar faltas o la congestión. Los protocolos de enrutamiento también necesitan hacer balanceo de la carga.
• ***Infraestructura Mesh con enrutamiento eficiente:*** Los protocolos de enrutamiento, se esperan que sean más simples que los protocolos de una red *ad hoc.* Con la infraestructura *Mesh* proporcionada por los *routers,* el protocolo de ruteo para clientes *Mesh* puede ser más simple. De acuerdo a estas características se recomienda el uso de MANET (Mobile ad hoc Networks) del IETF, que tiene dos tipos de protocolos: activos

como es el caso de AODV (Ad Hoc ondemand Distance Vector) y preactivos como es el OLSR (Optimizad Link State Routing).

Por otra parte, si los *routers Mesh* no tienen movilidad y sus rutas no varían tan dinámicamente, se pueden emplear otro tipo de protocolos, como el OSPF (Open Shortest Path First), con la extensión de movilidad que permita la autoconfiguración de la red, en el caso de que se caiga algún enlace.

Tipo de métricas funcionales: El impacto de la métrica del funcionamiento en un protocolo, es importante a la hora de seleccionar una trayectoria, según la métrica de la calidad del acoplamiento. Para esto se tienen en cuenta los siguientes tipos de ruteo:

• ***Enrutamiento de Multi-Radio:*** Un multi-radio LQSR es una nueva métrica que asume, que todas las radios en cada nodo, están asociadas a los canales que no interfieren con la asignación que cambia frecuentemente.

• ***Enrutamiento multidireccional:*** Los objetivos principales, con este tipo de enrutamiento es, el de hacer que una carga se balancee mejor y proporcionar alta tolerancia de avería. Las trayectorias múltiples se seleccionan entre la fuente y el destino. Cuando un acoplamiento está quebrado en una trayectoria, debido a una mala calidad o movilidad del canal, otra trayectoria, en el sistema de trayectorias existentes, puede ser elegida, sin esperar al una trayectoria nueva del enrutamiento. Sin embargo, dado un funcionamiento métrico, la mejora depende de la disponibilidad de las rutas entre la fuente y la destinación. Otra desventaja del enrutamiento multidireccional está en su complejidad.

• ***Enrutamiento Jerárquico****:* Este tipo de enrutamiento se emplea para agrupar nodos de red en "racimos". Cada racimo tiene a su vez una o más cabezas del racimo. Los nodos en un racimo pueden tener, uno o más saltos a una distancia lejana de la cabeza del racimo. Puesto que la conectividad entre los racimos es necesaria, algunos nodos pueden comunicarse con más de un racimo y trabajar como entrada. Cuando la densidad del nodo es alta, los protocolos del enrutamiento jerárquico, tienden a alcanzar un

funcionamiento mucho mejor, porque hay menos trayectoria y procedimiento y es más rápido debido la disposición de encaminar la trayectoria.

Sin embargo, la complejidad de mantener la jerarquía, puede comprometer el funcionamiento del protocolo de enrutamiento. Por otra parte, en WMNs, un cliente de acoplamiento, debe evitar ser una cabeza del racimo, porque puede convertirse en un embotellamiento debido a su capacidad limitada.

• ***Enrutamiento Geográfico:*** consiste en proyectar los paquetes delanteros, solamente usando la información de la posición de nodos en la vecindad y el nodo de destino. Así, el cambio de la topología tiene menos impacto en el enrutamiento geográfico, que los otros protocolos del enrutamiento. Los algoritmos geográficos, son un tipo de esquemas codiciosos del enrutamiento de una sola trayectoria, en los cuales la decisión de la expedición de paquete, se hace basándose en la información de la localización del nodo de la expedición, sus vecinos y el nodo de destino. Sin embargo, todos los algoritmos codiciosos del enrutamiento, tienen un problema común, es decir, la entrega no está garantizada aunque exista una trayectoria entre la fuente y el destino.

II.23.15.4. Capa de Transporte

Hasta el momento, no se ha propuesto ningún protocolo de transporte específicamente para WMNs. Sin embargo, una gran cantidad de protocolos de transporte están disponibles para las redes *ad hoc*. Estudiar estos protocolos ayuda en el diseño de los protocolos del transporte para WMNs.

Transporte confiable de los datos: Los protocolos confiables del transporte se pueden clasificar más a fondo en dos tipos: Variantes del TCP y nuevos protocolos del transporte. Las variantes del TCP, mejoran el funcionamiento del clásico TCP abordando los problemas siguientes:

• ***Pérdidas del paquete de la No-Congestión:*** El TCP clásico no puede distinguir las pérdidas de la congestión y la no congestión. Como resultado, cuando ocurren las

pérdidas de la no-congestión, el rendimiento de la red cae rápidamente debido a la evitación innecesaria de la congestión. Además, cuando los canales inalámbricos vuelven a la operación normal, el TCP clásico no se puede recuperar rápidamente. Se puede utilizar un mecanismo de regeneración, para distinguir diversas pérdidas del paquete.

• ***Falta desconocida del acoplamiento:*** La falta del acoplamiento ocurre con frecuencia en las redes *ad hoc* móviles, puesto que todos los nodos son móviles. Por lo que en las WMNs, la falta del acoplamiento no es tan crítica como en redes *ad hoc* móviles. Debido a los canales y a la movilidad inalámbrica en clientes de acoplamiento, la falta de acoplamiento inmóvil puede suceder.

• ***Asimetría de la red****:* La asimetría de la red se define, como situación en la cual la dirección delantera de una red, es perceptiblemente diferente de la dirección contraria, en términos de: anchura de banda, tarifa de la pérdida y estado latente. Así, afecta la transmisión de ACKs, puesto que el TCP es críticamente dependiente del ACK, su funcionamiento se puede degradar seriamente por asimetría de la red.

• ***Entrega en tiempo real:*** Para apoyar entrega *end-to-end* del tráfico en tiempo real, un protocolo del control de la tarifa (RCP) es necesario trabajar con el UDP. Aunque las RCPs se proponen para las redes atadas con alambre, no hay esquemas disponibles para WMNs.

II.23.15.5. Capa de Aplicación

Los usos apoyados por WMNs son numerosos y pueden ser categorizados en varias clases.

Acceso a Internet: Los usos variados del Internet proporcionan información oportuna, para hacer la vida más confortable y para aumentar eficacia y productividad en el trabajo. En un hogar o en un ambiente de negocio pequeño o mediano, la solución del acceso a la red más popular, es un módem inmóvil de DSL o de cable, junto con puntos de acceso IEEE 802.11. Sin embargo, comparado con este acercamiento, WMNs tiene

muchas ventajas potenciales: un costo más bajo, una velocidad más alta y una instalación más fácil.

Almacenaje y compartimiento de información distribuida: Tener acceso a *Backhaul* en Internet no es necesario en este tipo de uso y los usuarios se comunican solamente dentro de WMNs. Un usuario puede desear almacenar datos en grandes cantidades, en los discos poseídos por otros usuarios. En archivos de transferencia directa de los discos de otros usuarios, los cuales están basados en mecanismos de establecimiento de una red de par a par, los usuarios dentro de WMNs pueden también desear charlar, hablar en los teléfonos de video y jugar en línea con varias personas.

Intercambio de información a través de múltiples redes inalámbricas: Por ejemplo, un teléfono portátil puede desear hablar con otro usuario WiFi con WMNs, o un usuario en una red WiFi, puede esperar supervisar el estado de varios sensores, en redes de un sensor de la radio. Por lo tanto, hay principalmente tres direcciones de la investigación en la capa de uso.

Mejorar los protocolos de cada capa existentes que están en uso: En una red inalámbrica, los protocolos en las capas más bajas, no pueden proporcionar la ayuda perfecta para la capa que está en uso. Por ejemplo, según lo percibido por la capa de uso, la pérdida del paquete puede siempre no ser cero, el retraso del paquete puede ser variable. Estos problemas llegan a ser más severos en WMNs, debido a sus comunicaciones *ad hoc* y *multi-hop.* Tales problemas pueden ocasionar fallas en muchos usos del Internet, que trabajen en una red atada con alambre. Actualmente, muchos protocolos del par-a-par, están disponibles para la información que se comparte en el Internet. Sin embargo, estos protocolos no pueden alcanzar un funcionamiento satisfactorio en WMNs, puesto que WMNs tiene características mucho más diversas que el Internet.

II.23.16. Diferencias con otras Tecnologías

II.23.16.1. Redes WLAN tradicionales y redes Mesh

Una red WLAN tradicional, consta de uno o más puntos de acceso (AP) inalámbrico (Access Point), que se conectan mediante un cable UTP directamente a un *switch/hub Ethernet* hacia la red cableada. De esta misma manera, se podrían conectar más puntos de acceso para incrementar el área de cobertura de la red. Con las redes *WiFi Mesh*, es posible que estos puntos de acceso se puedan conectar y comunicar entre ellos de forma inalámbrica, utilizando las mismas frecuencias del espectro disperso, ya sea en 2.4 GHz o en la banda de 5.8 GHz.

Las redes *WiFi Mesh* son menos ambiciosas pero más reales y para operar sólo necesitan de clientes ordinarios IEEE 802.11. Las redes *WiFi Mesh* son simples, todos los puntos de acceso comparten los mismos canales de frecuencia. Esto hace a los APs relativamente baratos. El único problema es que el canal es compartido, es decir el ancho de banda de la red. Los APs actúan como *hubs,* así la malla funciona de manera similar a una red plana construida completamente de *hubs*; es decir todos los clientes contienden para acceder al mismo ancho de banda. Los sistemas multiradio, utilizan un canal para enlaces hacia los clientes WiFi y el resto para enlaces en malla hacia otros APs.

En la mayoría de las arquitecturas, los enlaces a los clientes están basados en 802.11b/g, debido a que la banda de frecuencia de 2.4 GHz, es la más utilizada por el hardware de los equipos WiFi. En cambio la red *Mesh* está basada en el estándar 802.11ª, debido a que la banda de 5 GHz está menos congestionada, habiendo menos riesgo de interferencia entre los enlaces de la malla y los clientes. Sin embargo, el estándar 802.11 no soporta las mallas, así que cada fabricante necesita implementar su propia tecnología propietaria por encima del 802.11a.

El estándar 802.11s, tiene la finalidad de reemplazar estas tecnologías propietarias, tanto para sistemas de un solo canal o de varios canales de radio.

Las redes *WiFi Mesh,* son útiles en lugares donde no existe cableado UTP, por ejemplo, oficinas temporales o edificios tales como bodegas o fábricas. Pero muchos de los fabricantes se están concentrando más bien en ambientes exteriores. En muchos lugares se ha incrementado el Internet público sobre redes WiFi, tales como aeropuertos o comercios. Quizá *WiFi Mesh* sea un modesto competidor de otra tecnología más madura conocida como ***WiMax.***

Un aspecto fundamental del funcionamiento de las redes *Mesh,* es que la comunicación entre un nodo y cualquier otro, puede ir más allá del rango de cobertura de cualquier nodo individual. Esto se logra haciendo un enrutamiento multisaltos, donde cualquier par de nodos que desean comunicarse, podrán utilizar para ello, otros nodos inalámbricos intermedios que se encuentren en el camino. Esto es importante si se compara con las redes tradicionales WiFi, donde los nodos deben estar dentro del rango de cobertura de un AP y solamente se pueden comunicar con otros nodos mediante los APs; estos APs a su vez, necesitan de una red cableada para comunicarse entre sí. Con las redes *Mesh*, no es necesario tener APs, pues todos los nodos pueden comunicarse directamente con los vecinos, dentro de su rango de cobertura inalámbrica y con otros nodos distantes mediante el enrutamiento multisalto ya mencionado.

II.23.16.2. Comparación entre redes inalámbricas Ad Hoc y redes Mesh

Entre las redes *ad hoc* y las redes *Mesh,* las principales diferencias son: la movilidad de los nodos y la topología de la red. Las redes *ad hoc* son redes de alta movilidad, donde la topología de la red cambia dinámicamente. Por otra parte, una red WMNs tiene una topología relativamente estable con la mayoría de los nodos fijos. Por lo tanto, la movilidad en redes *Mesh* es muy baja en comparación con las redes *Ad Hoc*.

Caracteristica	Red Ad Hoc	Red Mesh
Topologia de red	Altamente dinámica	relativamente estática
Movilidad de losnodos	De media a alta	Baja
Tiempo de servicio	Temporal	Semi permanente o permanente

Tipo de tráfico	Tráfico de usuario	Típicamente tráfico de usuario y tráfico de control de red
Ambientes deaplicación	Comunicaciones Internas	Comunicaciones internas y externas
Implementación	Fácil	Requiere algo de planificación

Tabla II.9 Comparación entre redes inalámbricas Ad Hoc y redes Mesh

Como se puede apreciar en la tabla, otra gran diferencia entre estos dos tipos de redes es el escenario de aplicación, ya que las redes *Mesh* son diseñadas para proveer servicios de comunicaciones a bajos costos, como ser: servicios de internet en zonas relativamente extensas como: ciudades, barrios, etc., mientras que las redes *ad hoc* se utilizan en ambientes pequeños.

II.23.17. Futuro de las redes Mesh

En los próximos años, la IEEE hará sus últimos esfuerzos por mejorar la estandarización de las redes *Mesh.* El establecimiento de una red *Mesh,* será asumido por los vendedores de los productos que incorporen el estándar 802.11s, con el fin de que el público adopte esta tecnología. Según estudios realizados en el 2006, se predice que la tecnología de redes *Mesh* será acogida en los próximos años, lo que garantiza que dichos productos esten muy pronto en el mercado, con el fin de satisfacer todas las necesidades de los clientes. Por otro lado, en el futuro se seguirán teniendo diversos tipos de tráfico en la red, por lo cual deberán realizarse distintas políticas, que permitan introducir Calidad de Servicio (QoS) en la red.

Los paquetes de voz deben tratarse con mayor prioridad, debe existir la posibilidad de priorizar siempre, algún flujo de tráfico especial para la activación de avisos o alarmas, ya sea mediante una comunicación de voz u otro mecanismo. También pueden introducirse mecanismos de control de congestión, de manera que se evite el envío de tráfico por rutas que se presenten muy saturadas y se aprovechen otros caminos posibles entre fuente y destino a través de la red *Mesh.* También deben evaluarse los distintos

tipos de hardware disponibles, para realizar funciones de encapsulado de la información, mediante interfaces y protocolos estándar, o bien, la realización de controladores específicos para los dispositivos necesarios.

II.23.18. Nuevas Aplicaciones y Escenarios

Tenemos escenarios conceptuales directamente aplicables a las nuevas WLAN Mesh, que se resumen a continuación:

II.23.18.1. Acceso a Internet de Banda Ancha

Los despliegues de redes de acceso con infraestructura cableada (última milla y nodos finales), resultan en muchas ocasiones impracticables, en términos de costes en zonas rurales y suburbios metropolitanos. Los operadores encuentran las siguientes barreras de inversión en estos casos:

- Costo-capital del equipamiento.
- Operación y mantenimiento de un número elevado de nodos.
- Despliegue de cableado en terrenos no urbanizados y de larga distancia.

A pesar de que las redes inalámbricas disminuyen considerablemente el coste de inversión, en la última milla de los operadores y proveedores de acceso a Internet, las redes *Mesh* solucionan esta situación, mejorando tanto el ancho de banda como los alcances mediante radioenlaces más cortos y de mayor densidad.

II.23.18.2. Red Mesh Comunitaria

Potenciando la idea de mejorar las relaciones, entre comunidades vecinas y áreas poblacionales más desfavorecidas a través de la tecnología, algunas ciudades están llevando a cabo, proyectos de acceso a Internet de bajo costo, vigilancia contra la delincuencia y redes de información vecinal mediante redes *Mesh*. En estos escenarios, los participantes son generalmente dueños del equipamiento y de la red *Mesh* y se

benefician de la compartición de accesos a través de diferentes tecnologías (cable, xDSL, WAN), la redundancia de accesos y el reparto del costo de tarificación.

II.23.18.3. Hogar Mesh

La nueva convergencia fijo-móvil, fomenta desarrollos paralelos en la electrónica del hogar; mediante la migración de funcionalidades *Mesh* a dispositivos cotidianos, pudiéndose establecer redes residenciales auto-configurables. Los dispositivos podrían descubrirse automáticamente de manera similar a la tecnología *plug-and- play*, capaces de establecer redes *Mesh* en el hogar, como: equipos de audio y vídeo (cámaras, TV, DVD, receptores de cable o satélite), teléfonos móviles y fijos, PDAs, Domótica del hogar (interruptores inteligentes, sistemas de inteligencia ambiental, etc).

II.23.18.4. Oficina Inalambrica

Las redes *Mesh* permiten establecer comunicaciones seguras y eficientes en entornos interiores de oficina, como lo son multitud de comercios. Si cada PC tuviese una tarjeta *WiFi Mesh,* se permitiría un despliegue rápido y de bajo coste, eliminando cables, *switches* y puntos de acceso adicionales. Esta opción representa una buena alternativa cuando la inversión en infraestructura cableada resulta demasiado alta.

II.23.18.5. Mesh Espontanea

La red *Mesh* espontánea se define como, el despliegue temporal de una red inalámbrica para la provisión de servicios de: voz, datos y vídeo, con el objetivo de colaborar activamente, en una situación local distribuida cuando no existe control centralizado ni infraestructura planificada previa.

II.23.18.6. Campus Mesh

Por sus características, existe otro escenario de aplicación que combina algunas de las peculiaridades de los anteriores. Se trata de los despliegues de redes *Mesh* en entornos de campus, ya sean parques tecnológicos, campus universitarios, etc.

II.24. Estándar IEEE 802.11s [68]

II.24.1. Introducción

Revisión del 802.11 del IEEE para redes *Mesh*, que está en estado de borrador. Define como se conectan dispositivos inalámbricos para formar una WLAN (Wireless Local Area Network) mallada o *Mesh.* Proporciona una arquitectura y protocolos que permiten el reenvió de tramas y la selección de camino en el nivel 2 (enlace de datos) del modelo OSI. 802.11s nació como Grupo de Estudio (Study Group) del IEEE 802.11 en el 2003 y se convirtió en Grupo de Trabajo (Task Group) en Julio de 2004.

Actualmente sigue en proceso de aprobación, la cual esta prevista para mediados de 2011, según las previsiones del IEEE. El enrutamiento se hace mediante HWMP (Hybrid Wireless Mesh Protocol). Este protocolo debe ser implementado obligatoriamente por todos los nodos *Mesh,* aunque se permite usar protocolos adicionales. La principal ventaja de este estándar, es que introduce un mecanismo de enrutamiento en la capa 2 (MAC), haciéndolo aparecer como un sistema LAN (802.x) para protocolos de capas superiores. Además, define aspectos como: acceso al medio, sincronización o seguridad y no solo cuestiones de enrutamiento *Mesh*. Pero el hecho de que el enrutamiento de IEEE 802.11s, funcione en la capa de enlace de datos, también se convierte en una desventaja, ya que de esta manera no podemos aprovechar, la estructura jerárquica de protocolos de direccionamiento superiores, como IP, ni interconectar diferentes redes.
Este hecho hace que, sea complicado enrutar paquetes solo con HWMP en redes *Mesh* de tamaño medio o grande, por ello se hace necesario combinar IEEE 802.11s con otros protocolos de capas superiores.

Existen tres implementaciones de IEEE 802.11s:

- Open 802.11s: implementación para el núcleo Linux a partir de la versión 2.6.26. Desarrollada por un consorcio empresarial formado por Nortel, Cozybit, OLPC (One Laptop per Child) y Google.

- Los equipos XO del OLPC: implementan 802.11s en las tarjetas de red inalambricas, permitiendo que el ordenador funcione como MP aunque el equipo este en modo *standby.*
- Wi_Mesh: implementaciónra sistemas FreeBSD desarrollada por dicha comunidad. Presente a partir de la versión 8.0. Es incompatible con la versión que incluye el núcleo Linux, ya que están basadas en versiones diferentes de protocolo.

II.24.2. Características

IEEE 802.11s es un proyecto de enmienda IEEE 802.11 para redes *Mesh*, que define cómo los dispositivos inalámbricos pueden interconectarse para crear una red WLAN *Mesh*, que puede ser usado para aplicaciones estáticas y topologías de redes *ad hoc*.

El estándar 802.11s es una propuesta del grupo de trabajo conocido como Wi-Mesh Alliance (www.wi-mesh.org). El borrador del estándar 802.11s define la capa física y enlace de datos para redes *Mesh*. Esta topología aumenta la cobertura de la red y permite estar siempre activa, aun cuando uno de los puntos de acceso falle. Se pueden agregar usuarios y puntos de acceso a la red para añadir capacidad, de la misma manera que la red Internet, la cual funciona en malla, también agregar nodos a la red, la hace escalable y redundante. El estándar ofrece la flexibilidad requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, campus, seguridad pública y aplicaciones militares. La propuesta se enfoca sobre múltiples dimensiones: la subcapa MAC, enrutamiento, seguridad y la de interconexión. El borrador especifica plataformas para equipos, de simples y múltiples canales de radio. También se especifica en algunos adendums, esquemas de priorización de calidad de servicio (802.11e), medición de recursos de radio (802.11k) y administración del espectro (802.11h).

La especificación también incluye características tales como: censado adaptativo de portadora, para re-uso espacial del espectro, coordinación de canales de acceso y soluciones de administración de recursos de radio frecuencia (RF). El 802.11s también provee características de: descubrimiento extendido de mallas con autoconfiguración automática y seguridad (802.11i). El estándar 802.11s, está centrado principalmente en

la capa 2, o capa de nivel de enlace de datos del modelo de referencia OSI. Para llevar a cabo la formación de redes *Mesh* inalámbricas, desarrolla funcionalidades tales como: descubrimiento de la red *Mesh,* autenticación, gestión de enlaces *Mesh*, selección de canal, seguridad, selección de ruta, *interworking* y control de congestión, entre otras.

II.24.3. Propósito general

802.11s es el estándar en desarrollo del IEEE para redes WiFi malladas *Mesh*. *Mesh* es una topología de red, en la que cada nodo está conectado a uno o más nodos, de esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. En los últimos años han surgido numerosos proyectos de implementación de redes WiFi Mesh.

El nicho en el que esta tecnología, parece haberse desarrollado de forma más espectacular, es el de la redes WiFi municipales, promovidas y financiadas por ayuntamientos, también denominadas *Metro WiFi*. Es un fenómeno que surgió inicialmente en Estados Unidos y que ha sido el 2006 su año de mayor desarrollo. Inicialmente estos sistemas se concibieron, como una forma económica de satisfacer las necesidades de comunicaciones de los ayuntamientos y de los servicios de emergencia, pero últimamente la utilización de WiFi se está planteando, como una alternativa gratuita o de bajo coste para proporcionar servicios de banda ancha.

II.24.4. Mejoras y funcionalidades específicas

Según la normativa 802.11 actual, una infraestructura WiFi compleja, se interconecta usando LANs fijas de tipo Ethernet. 802.11s pretende responder a la fuerte demanda de infraestructuras WLAN móviles con un protocolo para la autoconfiguración de rutas, entre puntos de acceso mediante topologías multisalto. Dicha topología constituirá un WDS (*Wireless Distribution System*), que deberá soportar tráfico: *unicast*, *multicast* y de *broadcast*. Para ello se realizarán modificaciones en las capas PHY y MAC de 802.11 y se sustituirá la especificación BSS (*Basic Service Set*) actual, por una más compleja conocida como ESS (*Extended Service Set*).

Aún no se conoce mucho de los detalles técnicos del estándar, pero parece que la redacción del mismo se está orientando de forma preferente, a dotar a la multitud de puntos de acceso aislados existentes en viviendas y oficinas, de la capacidad de conectarse con nodos exteriores pertenecientes a una red *Mesh* existente. De esta forma el grupo de trabajo, evitará que sus desarrollos se solapen con las avanzadas tecnologías desarrolladas desde hace años, por los fabricantes comerciales de redes *Mesh*, pero podrá hacer uso de las mismas, para ofrecer al usuario final, una plataforma estable desde la que pueda acceder a nuevas aplicaciones y servicios.

Otra ventaja añadida consiste en que, se mejorará la ocupación del espectro radioeléctrico urbano, al conectarse el cliente a su propio AP y no directamente al nodo exterior. Por último, se pondrá especial énfasis en que 802.11s, recoja las mejoras en cuanto a: tasa binaria, calidad de servicio y seguridad, que se incorporen en 802.11n, 802.11e y 802.11i, respectivamente.

II.24.5. Relación con las normas

802.11s depende de uno de los estándares: 802.11a, 802.11b, 802.11g ó 802.11n, para llevar el tráfico real. Uno o más protocolos de enrutamiento serán requeridos para la topología física de la red actual. 802.11s requiere (Hybrid Wireless Mesh Protocol, or HWMP), como protocolo por defecto. Sin embargo, otras *Mesh, ad hoc* o enrutamiento dinámico de estado de enlace (OLSR, BATMAN), pueden ser compatibles, incluso el enrutamiento estático (WDS, OSPF). La creación de redes *Mesh* a menudo implica acceso a la red de desconocidos, especialmente cuando una población visitante está siendo atendida. Así, el acompañamiento del estándar IEEE 802.11u, será requerido por la mayoría de las redes *Mesh,* para autenticar esos usuarios sin un registro previo o cualquier comunicación anterior en línea.

II.24.6. Situación del estándar y estado de desarrollo comercial

Los trabajos del grupo TGs están todavía lejos de su aprobación final. La petición de propuesta inicial para este protocolo, acabó en junio de 2005 con 15 propuestas, que

fueron reducidas progresivamente hasta acabar con dos, apoyadas por dos grupos distintos de empresas:

II.24.6.1. Propuesta Wi-Mesh

La "Wi-Mesh Alliance" (WiMA), cuyos miembros son Nortel, Philips, Accton, ComNets, InterDigital, NextHop, Extreme Networks, Laboratorio de Investigación de la Marina Estadounidense, Swisscom Innovations y Thomson, ofreció una propuesta que permitía a usuarios de tecnología inalámbrica, comunicaciones *seamless*, esto es, independencia de las aplicaciones de los procesos de traspaso de coberturas de radio y sus características son:

- Solución completa que permita todos los modelos de uso de IEEE 802.11s
- Soporte de configuración monoradio y multiradio.
- Eficiencia en términos de calidad de servicio (QoS).
- Auto configurable y fácil de operar.
- Ha de ser flexible y segura.
- Soporte de enrutamiento dinámico.
- Soporte de múltiples algoritmos de enrutamiento.
- Integración de la seguridad y enrutamiento.

Todas estas características proporcionan, flexibilidad operacional para el despliegue de redes, con equipos de diferentes fabricantes.

II.24.6.2. Propuesta SEEmesh

SEE (*Simple Efficient Extensible*) Mesh, liderada por Intel y apoyada por Nokia, Motorola, NTT DoCoMo y Texas Instruments, entre otras, cuya propuesta introducía como principal novedad los "*portales Mesh*", que ofrecerían interoperabilidad en redes *Mesh,* permitiendo que cualquier equipamiento WiFi ya existente, pudiera ser integrado en una red *Mesh*.

II.24.7. Estado Actual

No todos los proveedores que ofertan soluciones de redes *Mesh* propietarias, se han involucrado en el proceso de estandarización IEEE 802.11s. Algunos de los principales vendedores de tecnología *Mesh* actuales, entre los que se incluyen: BelAir Networks, Tropos Networks, RoamAD y Strix Systems, no son parte de ninguno de los grupos mencionados. En la reunión de enero de 2006, la selección de propuestas fue suspendida y las dos principales, "*SEEmesh"* y "*Wi-Mesh"* se unieron. La propuesta fusionada se presentó y aprobó unánimemente en la reunión de marzo de 2006, constituyendo la base del borrador IEEE 802.11s producido en noviembre de 2006.

La especificación propuesta, proporciona la arquitectura para WLAN Mesh escalables, adaptativas y seguras. Ofrece la flexibilidad necesaria para satisfacer, todos los modelos de uso contenidos en los entornos residenciales, oficina, campus, seguridad pública y militares; definiendo la subcapa MAC, el enrutamiento, la seguridad y la interacción de capas altas. El diseño soporta tanto plataformas monoradio como multiradio. De hecho, la función *Médium Coordination Function,* efectúa tres modos de operación, que permiten implementaciones simples y robustas, así como soluciones más sofisticadas para un rendimiento óptimo y mejor eficiencia espectral.

II.25. Protocolos para redes inalambricas Mesh [69], [70]

Según los modelos de la capa OSI y TCP/IP, la funcionalidad de la asignación de ruta está localizada en la capa 3, la capa de gestión de redes que normalmente usa el protocolo de Internet (IP). Hay esfuerzos para desarrollar protocolos de asignación de ruta, para las redes *Mesh* en la capa 2. Aunque esto "viola" el concepto de la capa red actual, se espera obtener los siguientes beneficios: acceso más rápido y más información del estado de la capa 2 y de la capa física.

El enrutamiento en capa 2 es más difícil de llevar a cabo, la información adicional sobre la estructura de la red, las direcciones IP no están disponibles en las direcciones MAC y es más difícil de hacer entre redes heterogéneas. No obstante, las ventajas del acceso a las capas más bajas, aumentarán la fiabilidad de las redes *Mesh* inalámbricas, debido a

las reacciones más rápidas y apropiadas a los cambios del ambiente, de los radio-canales. Los conceptos para la selección de la ruta son los mismos, tanto para la capa 3 o la capa 2, éstel último sólo usa las direcciones MAC. También significa que algunos mecanismos, hasta ahora desconocidos en capa 2, tengan que ser introducidos, como: tiempo de vida útil (TTL), dirección de la fuente y destino, como los saltos a través de la ruta inalámbrica *multihop.*

II.25.1. Métrica

La métrica, es el parámetro que se utiliza para determinar las prestaciones de las técnicas de enrutamiento y es particularmente útil para comparar diferentes alternativas. La primera métrica que se ha utilizado en redes *Mesh,* es el conteo de saltos (*hop counting*), ampliamente utilizada en la Internet cableada, per no es la más adecuada en redes inalámbricas, debido a la amplia desigualdad en las prestaciones de los saltos inalámbricos. Un "salto" se define como el trayecto entre dos *routers* adyacentes.

En una red inalámbrica, las pérdidas de paquetes, en un tramo entre dos *routers* pueden ser muy elevadas y es en general muy variable, dependiendo del presupuesto de potencia del enlace. En un enlace muy largo, las pérdidas tienden a ser mayores, por lo que a menudo un trayecto con varios radioenlaces cortos, puede presentar menos pérdidas que un trayecto con un solo enlace largo.

Una métrica que se presta mejor a las características de las redes *Mesh*, es la conocida como ETX (*Expected Transmisión Count*), basada en el conteo de los errores de transmisión esperados en el tramo. Esta técnica, desarrollada en MIT, ha sido aplicada a diferentes protocolos de enrutamiento en redes *Mesh*. Esto permite tomar en cuenta las características de transmisión de cada enlace, que se expresan con un "peso" o ponderación que se le asigna. Un enlace con mayores pérdidas tendrá una ponderación mayor, la que se utilizará para evaluar la métrica de la trayectoria total. Sin embargo, no toma en cuenta la posibilidad de que diferentes enlaces, puedan tener anchos de banda distintos, por lo que el tiempo de transmisión de un paquete, será menor en el enlace con

mayor ancho de banda. Esto ha motivado la propuesta de otra métrica, conocida como ETT (*Expected Transmisión Time),* en la que se multiplica ETX por el tiempo tardado en recorrer el respectivo tramo. Esto puede tener un impacto significativo, cuando los tramos considerados, incluyan diferentes puertas de enlace (*gateways*) a Internet, que pueden variar considerablemente en ancho de banda, o cuando se tengan tramos que utilizan 802.11 b, mezclados con tramos que utilizan 802.11 a ó g.

II.25.2. Requisitos de Enrutamiento en las Redes WMN

Un protocolo de asignación de ruta óptimo para redes WMNs, debe cumplir con lo siguiente:

- **Tolerancia a fallos:** Un problema importante en las redes es la supervivencia, que es la capacidad de la red para funcionar en caso de que un nodo falle. De la misma manera los protocolos de enrutamiento, también deberían permitir una nueva selección de ruta en caso de fallas.
- **Balanceo de carga:** Los *routers* inalámbricos *Mesh* son recomendados en el balanceo de carga, porque ellos pueden escoger la ruta más eficaz para los datos.
- **La reducción del enrutamiento Overhead:** La conservación del ancho de banda es indispensable para el éxito de cualquier red inalámbrica. Es importante reducir la asignación de ruta *overhead,* sobre todo el causado por la retransmisión.
- **Escalabilidad:** Una red *Mesh* es escalable y pueden ocuparse miles de nodos, ya que el funcionamiento de la red no depende de un punto o mando central.
- **QoS:** Debido a la limitada capacidad del canal, la interferencia es un factor muy importante. El gran número de usuarios y las aplicaciones multimedia en tiempo real, apoyada por la calidad de servicio (QoS), se ha vuelto un requisito indispensable en redes de computadoras.

II.25.2.1. Clasificación

La tarea principal de los protocolos de enrutamiento, es la selección del camino entre el nodo fuente y el nodo destino. Esto tiene que ser hecho de una manera confiable, rápida

y con gastos indirectos mínimos. En general, los protocolos de enrutamiento pueden ser clasificados en: los basados en topología y en los basados en posición. Los protocolos de enrutamiento basados en topología seleccionan trayectorias basadas en información topológica, como por ejemplo los enlaces de nodos.

Los protocolos de enrutamiento basados en posición, seleccionan trayectorias basadas en la información geográfica con algoritmos geométricos. Otras posibilidades para la clasificación de protocolos de enrutamiento son: *Flan* vs *hierarchical*, *distance vector* vs. *link state*, *source routing* vs. *hop-by-hop routing*, *single-path* vs. *multipath.* En principio las redes *Mesh* pueden manejar cualquier clase de protocolo de enrutamiento descrita anteriormente. Sin embargo no todo protocolo trabajará bien. La selección de un protocolo de enrutamiento conveniente, depende del: panorama, uso y requisitos de funcionamiento.

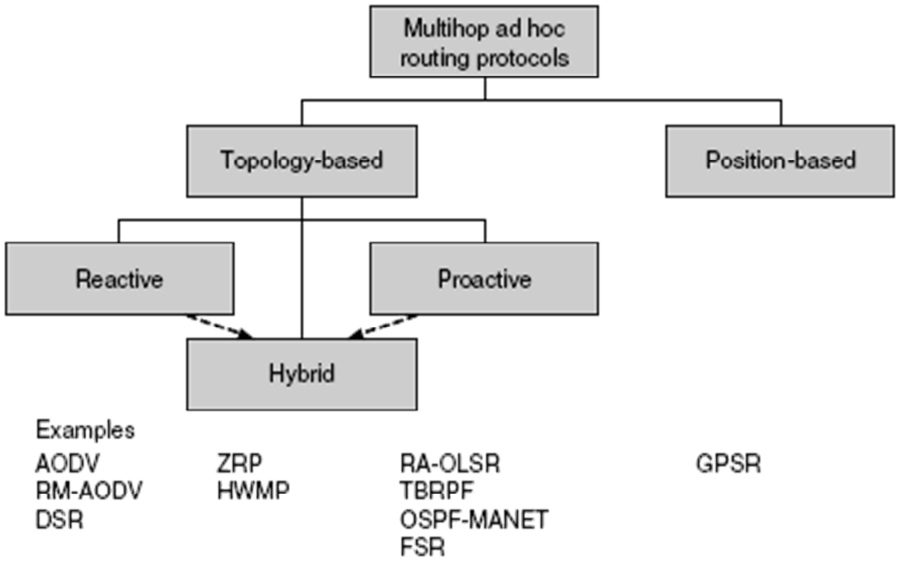

Figura II.28 Clasificación

Las redes WMNs, no dependen de infraestructura física, por lo que la comunicación viene dada por los sistemas de radio de los equipos. Para que se produzca esta comunicación entre los equipos, estos deben trabajar como *routers,* pero este enrutamiento es mucho más complejo que en las redes fijas. Este problema se intenta

resolver mediante un gran número de algoritmos y protocolos de enrutamiento. Hay un gran número de algoritmos, dado que esta tecnología está aún en investigación y se buscan soluciones desde vías muy diferentes, lo que da como resultado la aparición de un gran número de protocolos, los cuales se definen con características muy diferentes entren si.

II.25.2.1.1. Protocolos basados en topología (Topology based)

Los protocolos de enrutamiento basados en topología, son separados en 2 categorías que son llamados: reactivos, proactivos y los protocolos de enrutamiento híbrido. Los protocolos reactivos tales como AODV y DSR, inician la determinación de las rutas, solo si existe una petición. Esto quiere decir que la información de la ruta, solo está disponible cuando se recibe una petición, utilizando este tipo de implementaciones, pueden existir retardos significativos antes de que la ruta de destino pueda ser determinada. También será necesario hacer cierto control de tráfico mientras se busca la ruta. En los protocolos proactivos como OLSR y DSDV, intentan establecer todas las rutas con la red. Esto significa que cuando se necesita una ruta, esta ya es conocida y puede usarse de forma inmediata.

II.25.2.1.1.1. Reactivo o bajo demanda

Un protocolo de enrutamiento puede mantener la información bajo demanda (reactivo), es decir, actualiza su información de enrutamiento a medida que es necesaria. Este tipo de protocolo no necesita, que todos los nodos tengan la información de enrutamiento en todo momento, sino que la actualizará a medida que la necesita. Lo que se pretende conseguir es que la red inalámbrica, no tenga una gran carga de señalización innecesaria. Se puede considerar muy útil cuando la información viaja a menudo por rutas muy parecidas. Estos protocolos necesitan saber al menos el primer salto que deben hacer, si no lo conocen se debe hacer un *broadcast* hacia todos los nodos vecinos, esta estrategia sólo se puede utilizar en los primeros saltos, si se utilizara en exceso se inundaría la red, lo que no es conveniente. Los paquetes no se empiezan a enviar hasta que la ruta no esté

especificada, esto supone un retraso en el envío de los primeros paquetes. Una vez que la ruta está finalizada, se debe guardar en caché, la tabla de enrutamiento durante un período de tiempo, una vez que pasa ese tiempo, la ruta se invalida.

II.25.2.1.1.1.1. AODV (Ad Hoc On-Demand Distance Vector)

Este protocolo permite el enrutamiento dinámico, autoarranque y *multihop,* entre todos los nodos móviles que participan en la red. AODV permite a todos los nodos obtener las rutas rápidamente para nuevos destinos y no requiere que los nodos mantengan las rutas hacia los destinos que no están activos en la comunicación. El protocolo de enrutamiento está diseñado para redes móviles *ad hoc* con gran cantidad de nodos y con distintos grados de movilidad.

Este protocolo se basa, en que todos los nodos tienen que confiar en los otros para transportar sus datos, utilizando mecanismos para evitar la participación de nodos intrusos. Una característica distintiva de este protocolo, es el uso del número de secuencia para cada ruta. Este número de secuencia es creado por el nodo destino para ser incluido con la información necesaria, para los nodos que requieren la información. El uso de estos números de secuencia, implica que no se creen bucles y se facilite la programación.

Una particularidad de AODV, es la reparación a nivel local de un enlace caído que forma parte de una ruta activa. En este caso, el nodo que detecta la caída de un enlace que esta siendo utilizado, procede a intentar repararlo, comenzando con un proceso de descubrimiento de ruta hacia el destino y coloca en cola los paquetes de datos recibidos para el destino, hasta localizar una nueva ruta. En el caso de que este intento resulte fallido, se dará lugar al proceso normalmente establecido, con el envío del mensaje de error **RERR** hacia el nodo origen.

II.25.2.1.1.1.2. DSR (Dynamic Source Routing)

El protocolo DSR se fundamenta en el enrutamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información, acerca de los nodos exactos que deben atravesar. No requiere ningún tipo de mensajes periódicos (reactivo), disminuyendo así la sobrecarga con mensajes de control. Además ofrece la posibilidad de obtener, con la solicitud de una ruta, múltiples caminos posibles hacia el destino.

Para poder realizar el enrutamiento en el origen, a cada paquete de datos se le inserta una cabecera DSR de opciones, que se colocará entre la cabecera de transporte y la IP. Entre dichas opciones se incluirá la ruta que debe seguir el paquete nodo a nodo. Cada nodo mantiene una memoria caché de rutas, en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de rutas, ya sean propios u obtenidos a través de escuchas en la red.

II.25.2.1.1.2. Proactivo o basado en tablas

Son aquellos en los que los algoritmos mantienen en cada nodo, información actualizada acerca de la topología de la red, la cual es almacenada en tablas de enrutamiento, que son actualizadas de forma periódica u originada por eventos. Este tipo de protocolos están basados en los protocolos de “vector distancia” y de “estado de enlace”. Los protocolos proactivos, al contrario que los reactivos (bajo demanda), intentan mantener toda la información de enrutamiento correcta, en todos los nodos de la red y en cada momento.

Estos protocolos también se pueden dividir en dos clases: los que tratan eventos y los que se actualizan de manera regular. Los que trabajan con eventos, no envían paquetes de actualización hasta que no hay un cambio en la topología de la red. En cambio, en el caso de actualización regular, la información se retransmite cada cierto tiempo. La ventaja de este tipo de protocolos, es que no necesitan un tiempo para crear la ruta, por el contrario añaden mucha más carga a la red.

II.25.2.1.1.2.1. OLSR (Optimized Link State Routing Protocol)

El protocolo *Optimized Link State Routing* (**OLSR**) es un mecanismo estándar de enrutamiento pro-activo, que trabaja en forma distribuida para establecer las conexiones entre los nodos en una red inalámbrica *ad hoc* (*mobile ad hoc networks*, MANETs). Este protocolo fue diseñado en un principio por el Instituto Nacional Francés de Investigación en Informática y Automática (INRIA) y ha sido posteriormente estandarizado por el *Internet Engineering Task Force* (IETF).

OLSR es un protocolo para *Wireless ad hoc netwoks*. Este protocolo desarrollado para redes móviles *ad hoc*, opera en modo proactivo. Cada nodo selecciona un grupo de nodos vecinos como "*multipoint relay*" (MPR), en este caso sólo los nodos seleccionados como tales, son responsables de la retransmisión de tráfico de control. Estos nodos también tienen la responsabilidad de declarar, el estado del enlace a los nodos que los tienen seleccionados como MPR. Es muy útil para redes móviles densas y grandes, porque la optimización que se consigue con la selección de los MPR, trabaja bien en estos casos. Cuanto más grande y densa sea una red, mejor es la optimización que se consigue con este protocolo. OLSR utiliza un enrutamiento salto a salto, es decir, cada nodo utiliza su información local para enrutar los paquetes.

II.25.2.1.1.3. Protocolos Híbridos

Los protocolos de enrutamiento híbridos, tratan de combinar las ventajas de las 2 filosofías anteriores. Proactivo es usado para nodos o para caminos cercanos, mientras que el enrutamiento reactivo es usado para nodos lejanos y por lo general para caminos o rutas menos usados.

II.25.2.1.1.3.1. Hybrid Wireless Mesh Protocol (HWMP)

HWMP es el protocolo de enrutamiento por defecto, para el establecimiento de una red Mesh WLAN. Cada dispositivo que es regido por IEEE 802.11s, será capaz de usar este protocolo de enrutamiento. La naturaleza híbrida y la flexibilidad de configuración de HWMP, proporcionan un buen funcionamiento en todos los panoramas anticipando su

uso. La realización de HWMP, es una adaptación de ruteo reactivo al protocolo AODV, a la capa 2 y a la métrica *radio-aware,* llamada la radio métrica AODV (RM-AODV).

Un nodo *Mesh,* generalmente un portal *Mesh,* puede ser configurado periódicamente anunciando una difusión, que es fijado en la cima, la cual permite el ruteo proactivo hacia este portal *Mesh.* La parte reactiva de HWMP sigue los conceptos generales de AODV, según se ha descrito antes. El protocolo HWMP utiliza el método de vector distancia y el proceso de descubrimiento de la ruta, con la petición de la ruta y su respuesta respectiva. Los números de serie de la destinación, se utilizan al reconocer la vieja información de ruteo. Sin embargo, hay significativas diferencias en los detalles.

HWMP utiliza direcciones MAC como protocolo de ruteo para la capa 2, en vez de direcciones IP. Además, HWMP puede hacer uso de una métrica de ruteo más sofisticada que el *hopcount*, tal como: métricas *radio-aware*. Un campo métrico de la nueva trayectoria, es incluida en los mensajes de RREQ/RREP, que contiene el valor acumulativo de los enlaces métricos de la trayectoria hasta el nodo destino. El ruteo por *default* métrico de HWMP, es el *airtime* métrico, donde las métricas separadas del enlace se agregan, hasta conseguir la trayectoria métrica.

Función

HWMP describe un método para conectar los elementos de una red inalámbrica *Mesh.* La característica de una red *Mesh,* es que los elementos de la red no necesitan ser estáticos. Las conexiones tienen que adaptarse en mayor o menor disponibilidad, independiente de los nodos de control y las intensidades de señales variadas.

Método

Está compuesto por un modo reactivo y otro proactivo, permitiéndose un funcionamiento individual y también de ambos modos en conjunto. HWMP utiliza"enrutamiento reactivo". Lo que hace la red "híbrida" es que también tiene elementos "proactivos". El enrutamiento reactivo no tiene un mapa de la red

disponible.Un "*Path Request*" (PREQ) es un paquete enviado cada vez que una ruta es necesitada.

Todos los nodos de la red, pasan la solicitud hasta que se alcance el destino deseado. El nodo responde y el camino se utiliza para formar una conexión. El enrutamiento reactivo da una gran flexibilidad para la creación de redes *Mesh,* donde los nodos son móviles (aplicaciones de emergencia y militares). El enrutamiento proactivo reduce la carga de tráfico de control *intra-mesh,* en redes con nodos fijos.

II. 25.2.1.2. Protocolos basados en posición (position-based)

Esta clase de algoritmos de enrutamiento, son paquetes enviados, basados en la posición geográfica del nodo al que se quiere llegar, sus nodos vecinos y el nodo destino. Estos protocolos requieren que cada nodo conozca su posición geográfica. La posición del nodo destino ha de ser dada por un servicio de ubicación, es un algoritmo simple de búsqueda, como el *greedy forwarding,* que puede ser usado para obtener información de la posición. El paquete se envía al vecino más cercano del nodo destino. Sin embargo el algoritmo simple de búsqueda, puede acercarse pero no alcanzar el nodo destino, aunque exista un enlace con el destino, según lo ilustrado en la Figura II.29

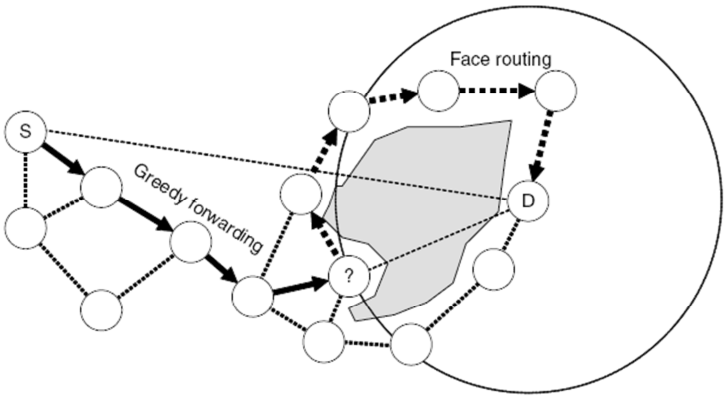

Figura II.29 Protocolos basados en posición (position-based)

II. 25.2.1.2.1. GPSR

Uno de los primeros protocolos de enrutamiento, basado en una posición práctica para las redes inalámbricas, es el *Greedy Perimeter Stateless Routing*, mas conocido por sus siglas como GPSR. El GPSR combina el *greedy forwarding* con el *fase routing fallback*. GPSR, es un protocolo que reacciona rápidamente, además es un eficiente protocolo de enrutamiento para redes móviles inalámbricas.

Este algoritmo, es distinto a los algoritmos de enrutamiento antes mencionados, que utilizan nociones gráfico-teóricas de las trayectorias más cortas y de la capacidad transitiva para encontrar las rutas. GPSR explota la relación entre la posición y la conectividad geográfica en una red inalámbrica, usando las posiciones de nodos para tomar decisiones con respecto al *forwarding* de los paquetes. GPSR utiliza *greedy forwarding* para remitir los paquetes a los nodos que están siempre progresivamente más cercanos al destino.

En las regiones de la red donde no existe un camino *greedy*, GPSR se recupera por la búsqueda en en el modo perímetro, en el cual un paquete atraviesa caras sucesivas más cercanas del gráfico de radio completo, en la conectividad de la red, hasta alcanzar un nodo más cercano al necesitado (nodo destino), donde el *greedy forwarding* termina. GPSR permitirá la construcción de las redes, que no pueden escalar con los algoritmos anteriores del enrutamiento para las *wired networks* y *wireless network.* Tales clases de redes incluyen:

- **Rooftop networks**: (Redes del tejado) despliegue fijo, denso en números extensos de nodos.
- **Redes ad hoc**: densidad móvil, que varía, sin ninguna infraestructura fija
- **Redes del sensor**: densidad móvil, potencialmente grande, números extensos de los nodos, recursos empobrecidos del per-nodo.
- **Redes de vehículos**: densidad móvil, sin energía obligada, movilidad.

Esta nueva tecnología permite desdoblar la transmisión de voz y datos, en diferentes canales que transmiten de forma paralela, permitiendo mantener conversaciones, sin cortar la transmisión de datos. En GPSR se puede elegir entre varios canales, de forma similar a como se realiza en Internet. El aumento de la velocidad se produce, porque los datos se comprimen y se envían a intervalos regulares, llamado "conmutación por paquetes", lo que aprovecha mejor la banda de frecuencia.

II.26. Fabricantes de dispositivos para redes Mesh [71]

La *Wi-Mesh Alliance* es un grupo de compañías, cuyo objetivo consiste en establecer con rapidez un estándar para WLANs *Mesh*, que permita una comunicación fluida entre los usuarios de dispositivos inalámbricos, no obstante el proveedor del equipo. La propuesta de la Wi-Mesh Alliance, se desarrolló de acuerdo con los lineamientos de la asociación de estándares IEEE, asi mismo, se basa en los protocolos 802.11 pendientes, para permitir la reutilización y la compatibilidad de tecnología.

A continuación se muestra una tabla, con los principales fabricantes de equipos, para implementaciones de redes *Mesh,* que prioriza el enfoque del producto en función de los principales mercados a los que va dirigido.

Principales fabricantes de WI-FI Mesh				
Tipo de red	**Radios por router**	**Frecuencia**	**Enlace del cliente**	**Fabricante**
MAN	1,2 o 4	5GHz	802.11b/g	BelAir Networks
MAN/LAN	2	2,4GHz, 5GHz	802.11b/g/n	Cisco Systems
MAN/LAN	1	2.4GHz, 5GHz	Ethernet	Firetide
MAN	2	5GHz	802.11b	Nortel Networks
MAN/LAN	2 a 6	2.4GHz, 5GHz	802.11a/b/g, bluetooth	Strix Systems
MAN	1	2,4GHz	802.11b/g	Tropos Networks
LAN	1 o mas	2.4GHz, 5GHz	802.11a/b/g/n	802.11s

Tabla II.10 Fabricantes de dispositivos para redes Mesh

Target Wireless Mesh Markets by Vendor

Vendor	Metro Mesh	Public Safety	Enterprise	Digital Divide	Mobile Mesh
BelAir	1	2	3	3	4
Firetide	3	3	1	4	4
Hopling	1	4	4	4	4
Locust World	4	4	4	1	4
CUWiN	4	4	4	1	4
MeshDynamics	1	3	3	3	4
Motorola	2	1	4	3	1
Nortel	1	2	3	4	2
PacketHop	4	1	4	4	1
RoamAD	1	4	4	2	4
Strix	2	3	1	4	4
Tropos	1	2	3	3	4

Source: *Unstrung Insider*

Key:

1	Primary target: The major target market or application for this vendor
2	Secondary target: An important target market for this vendor
3	Tertiary target: Nice-to-have-business
4	Not targeted: The vendor has not developed a product for this application

Figura II.30 Fabricantes de dispositivos para redes Mesh

II.26.1. Cisco Systems

Cisco Systems, uno de los fabricantes de equipos de comunicación más importante a nivel mundial, encontró la respuesta a la necesidad de extender las comunicaciones WiFi, de una manera sencilla, segura, en tiempo real y muy eficiente en costes, lanzando al mercado sus nuevas soluciones de próxima generación, basadas en tendencias *Wireless 2.0*, donde ciudades y empresas estarán conectadas. Las nuevas soluciones de Cisco, tanto para entornos interiores como exteriores con funcionalidad *Mesh*, son la última incorporación a la cartera de productos inalámbricos de ésta compañía.

La solución inalámbrica *Mesh* de Cisco Systems, permite ofrecer servicios innovadores como: implementar una red *Mesh* municipal o comunitaria; siendo útiles para administradores de: locales, agencias de viajes con varias sucursales, agencias de transporte, entre otras. Entre las características principales de la red *Mesh* de Cisco Systems tenemos:

- Permite una comunicación flexible, móvil y dinámica.
- Es una alternativa de bajo coste en ambientes donde no se puede tender cable.

- Fácil de añadir nodos y dispositivos a la red.
- Permite la integración con tecnología de red existente.
- Ofrece seguridad a lo largo de la red.

II. 26.2. BelAir Networks

BelAir Networks, define una red *Mesh* como una aplicación inalámbrica, en la cual se tiene una amplia flexibilidad en los enlaces que se pueden ofrecer con esta tecnología. Los enlaces a su vez pueden ser: Punto a Punto, Punto a Multipunto y Multipunto a Multipunto. Según *BelAir Networks* las características principales de una red *Mesh* son:

- Topología arbitraria de nodos y conectividad entre ellos.
- Enrutamiento del tráfico de forma autómata.
- Múltiples puntos de entrada/salida.

Además considera que una red *Mesh*, debe ser aplicable en áreas donde se desea repartir servicios de red de forma inalámbrica, típicamente en áreas grandes (ciudades, campus, puertos, entre otras), donde se necesita transportar gran cantidad de información y tener servicios con una respuesta rápida y sin que exista pérdidas de comunicación, tales como: datos, voz y video.

II.26.3. Firetide

Firetide es una empresa de tecnología inalámbrica especializada en redes *Mesh,* que desarrolla equipamiento con altas prestaciones, escalabilidad y de fácil instalación. La solución es idónea para construir infraestructura *backbone*, para redes WiFi, HotZones de acceso a Internet, video-vigilancia y redes temporales, en una variedad de entornos como pueden ser: aeropuertos, hoteles, campus y otras áreas donde es muy difícil o muy cara la instalación por cable.

Firetide, líder en conexiones de redes *Mesh* inalámbricas, ha creado el software de administración de *Mesh HotView Pro*(TM), para proveedores de servicio y grandes

empresas, ofreciendo una escalabilidad *Mesh* de hasta 1.000 nodos y la capacidad de desplegar y administrar numerosos entornos *Mesh*.

II. 26.4. Tropos Networks

Combinando la cobertura ubicua del celular, con la facilidad y la velocidad del WiFi, las redes de Tropos produjeron la primera arquitectura de *MetroMesh,* que es capaz de proporcionar rentabilidad y seguridad, entregando datos de banda ancha a los clientes estándares WiFi, en las áreas de la cobertura que atraviesan *hot-spots o hot-zones*, en metro-áreas enteras. La arquitectura de *Tropos MetroMesh* proporciona la flexibilidad máxima en la instalación y la capacidad de reaccionar y de responder a las fallas sin interrupción del *backhaul* inalámbrico, debido a los factores tales como: interferencia o pérdida de un acoplamiento atado con alambre del *backhaul,* con un mínimo de intervención del operador.

Las herramientas del análisis y del control de *Tropos MetroMesh* reducen al mínimo el planeamiento de red, el despliegue y costos de la gerencia. Las herramientas del análisis y del control de Tropos MetroMesh, fueron diseñadas para dar a operadores de red, centralización y visibilidad en todos los aspectos del funcionamiento de la red. Además permite el análisis, la optimización y el control de los sistemas altamente dispersados del acoplamiento. Cabe destacar que *Tropos Network* es el fabricante con mayores ventas en el mundo.

II. 26.5. Motorola

Motorola tiene también su solución *Mesh* que la denomina *MOTOMESH Duo*, la cual es considerada como una solución poderosa y de última generación para redes *Mesh* de radios duales. Con la ayuda de los productos de MOTOMESH y la tecnología de banda ancha inalámbrica, solida y a prueba de obsolescencia que tiene Motorola, se hace posible que existan ciudades inalámbricas, proporcionando acceso inalámbrico a: complejos industriales, educacionales, empresas, barrios o ciudades.

II. 26.6. Skypilot

Skypilot con sede en Silicon Valley (California), es proveedor de banda ancha inalámbrica *carrier-class*. Sus diferentes productos permiten desplegar de manera rápida y eficiente, una red por la que el usuario podrá utilizar servicios de VoIP, videovigilancia y servicio WiFi público. Sus soluciones ofrecen un alto ROI y técnicamente permiten hacer enlaces de larga distancia. *Skypilo*t utiliza el protocolo TDD (Time Division Duplex), el cual es el encargado de sincronizar todas las transmisiones para maximizar el rendimiento. Usando el sistema de localización global (GPS), la tecnología SyncMesh coordina las transmisiones simultáneas a través de la red *Mesh.* Su estrategia está enfocada a dotar de cobertura WiFi a grandes áreas como pueden ser un municipio.

Skypilot se caracteriza por la utilización en sus diferentes nodos, de un arreglo de 8 antenas para conseguir mejores zonas de cobertura y capacidades superiores a sus competidores. Su tecnología está patentada y es miembro del foro WiMAX. El despliegue de SkyPilot requiere una huella mínima, sacando ventaja de la estructura municipal existente, como azoteas de edificios o postes de alumbrado público para lograr un costo efectivo del despliegue. Ninguna otra solución *Mesh i*nalámbrica puede soportar el rango de aplicaciones en demanda de los municipios y de proveedores de servicio con esta combinación de facilidad de proporción y flexibilidad.

II.26.7. Nortel

La solución Wireless Mesh Network de Nortel, se ha implementado en empresas, universidades y agencias gubernamentales, tales como las ciudades de Taipei y Kaohsiung en Taiwán, la Universidad de Arkansas, la Universidad Edith Cowan en Australia, y la Universidad Seo Won y el Black Stone Golf & Resort en Corea. La propuesta de diseño de la Wi-Mesh Alliance pretende ser compatible con las modificaciones futuras al rendimiento 802.11n.

Nortel tiene negocios en más de 150 países**.** Nortel proporciona una entrada de valor añadido en el negocio sin hilos de alta velocidad del paquete y de los datos, ofrece el acceso inalámbrico de alta velocidad de los datos del paquete, a través de un área más amplia de cobertura, es muy económico ya que los algoritmos de la autoconfiguración en puntos de acceso sin hilos, eliminan los costes asociados a la ingeniería y a la organización de la red sin hilos del *backhaul*.

Esta solución puede utilizarse tanto en interiores como en exteriores y resulta ideal para ambientes extensos y de amplia cobertura, como empresas, universidades, fábricas, centros comerciales, aeropuertos, lugares de diversión y eventos especiales, operaciones militares, instalaciones temporales, seguridad pública y municipalidades, incluyendo centros de ciudades, áreas residenciales, parques y servicios de transporte en áreas públicas o comunidades residenciales.

II.27. Redes Virtuales LAN (VLAN) [72], [73], [74], [75], [76], [77], [78]

Una **VLAN** (acrónimo de *virtual LAN*, «**red de área local virtual**») es un método de crear redes lógicamente, independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el tamaño del dominio de *broadcast* y ayudan en la administración de la red, separando segmentos lógicos de una red de área local, que no deberían intercambiar datos usando la red local.

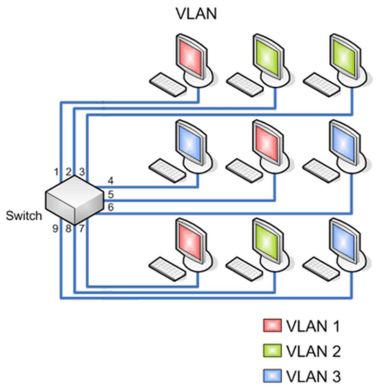

Figura II.31 Redes Virtuales

Una VLAN consiste en una red de ordenadores, que se comportan como si estuviesen conectados al mismo switch, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs, mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge, cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

II.27.1. Protocolos y diseño

El protocolo de etiquetado IEEE 802.1Q, domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (*Inter-Switch Link*) de Cisco, una variante del IEEE 802.1Q, y el VLT (*Virtual LAN Trunk*) de 3Com. Los primeros diseñadores de redes enfrentaron el problema del tamaño de los dominios de colision (Hubs), esto se logró controlar a través de la introducción de los switch o conmutadores, pero a su vez se introdujo el problema del aumento del tamaño de los dominios de *broadcast* y una de las formas más eficientes para manejarlo fue la introducción de las VLANs.

Las VLANs también pueden servir para restringir el acceso a recursos de red, con independencia de la topología física de ésta, si bien la robustez de este método es discutible, al ser el salto de VLAN (*VLAN hopping*) un método común de evitar tales medidas de seguridad. Las VLANs se caracterizan en el nivel 2 (enlace de datos) del modelo OSI, sin embargo, los administradores suelen configurar las VLAN como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

Un *router* (*switch* de nivel 3) funciona como «columna vertebral», para el tráfico de red transmitido entre diferentes VLAN. En los dispositivos Cisco, el protocolo VTP (*VLAN Trunking Protocol*) permite definir dominios de VLAN, lo que facilita las tareas

administrativas. VTP también permite «podar», lo que significa dirigir tráfico VLAN específico solo a los switches que tienen puertos en la VLAN destino.

II.27.2. Gestión de la pertenencia a una VLAN

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLAN estáticas y VLAN dinámicas. Las VLAN estáticas también se denominan VLAN basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un *switch* o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN ha la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el *switch.* En las VLAN dinámicas, la asignación se realiza mediante paquetes de software, el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática, basándose en información tal como, la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN.

II.27.3. Tipos de VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

II.27.3.1. VLAN Estáticas

Los puertos del *switch* están ya preasignados a las estaciones de trabajo. Dentro de la asignación de VLAN estáticas tenemos:

VLAN de nivel 1 (también denominada *VLAN basada en puerto*) Define una red virtual según los puertos de conexión del s*witch*.Se configuran por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Ventajas:

- Facilidad de movimientos y cambios.
- Microsegmentación y reducción del dominio de *Broadcast.*
- Multiprotocolo: La definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

- Administración: Un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del *switch* al que esta conectado el usuario. Esto se puede facilitar combinando con mecanismos de LAN Dinámicas.

VLAN de nivel 2 (también denominada *VLAN basada en la dirección MAC*) Define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

Ventajas:

- Facilidad de movimientos: No es necesario, en caso de que una terminal de trabajo cambie de lugar, la reconfiguración del *switch.*
- Multiprotocolo.
- Se pueden tener miembros en múltiples VLANs.

Desventajas:

- Problemas de rendimiento y control de *Broadcast*: el tráfico de paquetes de tipo *Multicast* y *Broadcast* se propagan por todas las VLANs.
- Complejidad en la administración: En un principio todos los usuarios se deben configurar de forma manual, las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

VLAN de nivel 3: existen diferentes tipos de VLAN de nivel:

VLAN basada en la dirección de red: Conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los s*witches* cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

Ventajas:

- Facilidad en los cambios de estaciones de trabajo: Cada estación de trabajo, al tener asignada una dirección IP en forma estática, hace innecesario reconfigurar el switch.

Desventajas:

- El tamaño de los paquetes enviados es menor, que en el caso de utilizar direcciones MAC.
- Perdida de tiempo en la lectura de las tablas.

VLAN basada en protocolo: Permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos, que utilizan el mismo protocolo en la misma red.

Ventajas:

- Segmentación por protocolo.
- Asignación dinámica.

Desventajas

- Problemas de rendimiento y control de *Broadcast:* Por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.
- No soporta protocolos de nivel 2 ni tampoco dinámicos.

II.27.3.2. VLAN Dinámicas (DVLAN)

Las VLANs dinámicas son puertos del *switch* que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN, el *switch* confirma la dirección MAC, ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual le corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN, es el menor trabajo de administración dentro del armario de comunicaciones, cuando se cambian de lugar las estaciones de trabajo o se agregan mas y también la notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

II.27.4. Ventajas de la VLAN

La VLAN permite definir una nueva red por encima de la red física y por lo tanto ofrece las siguientes ventajas:

- **Mayor flexibilidad en la administración y en los cambios de la red**: Ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores.
- **Seguridad:** Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- **Reducción de costo**: El ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.
- **Mejor rendimiento**: La división de las redes planas de Capa 2, en múltiples grupos lógicos de trabajo (dominios de broadcast), reduce el tráfico innecesario en la red y potencia el rendimiento.
- **Mitigación de la tormenta de broadcast**: La división de una red en las VLAN, reduce la cantidad de dispositivos que pueden participar en una tormenta de

broadcast. La segmentación de LAN, impide que una tormenta de broadcast se propague a toda la red.

- **Mayor eficiencia del personal de TI**: Las VLAN facilitan el manejo de la red, debido a que los usuarios con requerimientos similares de red, comparten la misma VLAN. Cuando proporciona un *switch* nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular, se implementan cuando se asignan los puertos.
- **Administración de aplicación o de proyectos más simples**: Las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos geográficos o comerciales. Tener funciones separadas hace que, gestionar un proyecto o trabajar con una aplicación especializada sea más fácil.

II.27.5. Aplicaciones y productos

Puntos en que las redes virtuales pueden beneficiar a las redes actuales:

- ***Movilidad:*** El punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.
- ***Dominios lógicos:*** Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.
- ***Control y conservación del ancho de banda:*** Las redes virtuales pueden restringir los *broadcast* a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo, no reduce el ancho de banda disponible para el mismo, ni para otros.
- ***Conectividad:*** Los modelos con funciones de *routing,* nos permiten interconectar diferentes *swtiches* y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

- ***Seguridad:*** Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.
- ***Protección de la inversión:*** Las capacidades VLAN están, por lo general, incluidas en el precio de los *switches* que las ofrecen y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.

CAPITULO III

SITUACION ACTUAL DE LA RED DE LA UPDS

CAPITULO III

Situación Actual de la Red de la UPDS

III.1. La Universidad Privada Domingo Savio (UPDS)

III.1.1. Ubicación

La Universidad Privada Domingo Savio se encuentra ubicada en la ciudad de Tarija, localizada al sur de Bolivia. La ciudad de Tarija es la capital de la provincia Cercado y del Departamento del mismo nombre. La Universidad Privada Domingo Savio se encuentra ubicada exactamente al suroeste de la ciudad, su ubicación geográfica es 21°32’12.20”S y 64°44’29.71”O.

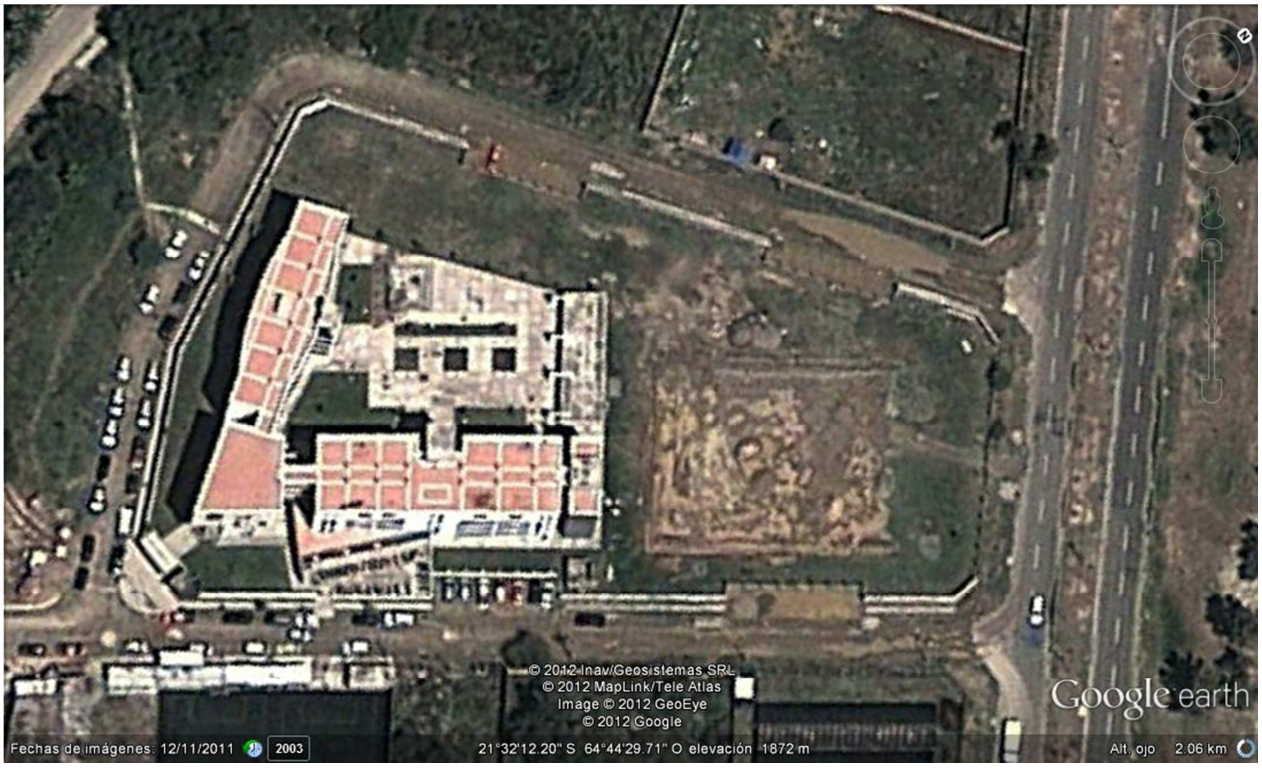

Figura III.1 Vista de la UPDS

III.1.2. Antecedentes

La propuesta de ampliar la cobertura de la red de la UPDS, viene tomando importancia debido al crecimiento de la población estudiantil y de los requerimientos que tiene la Universidad, donde tanto estudiantes como docentes, se ven en la necesidad de tener

acceso a la red e Internet para poder facilitar el proceso de enseñanza-aprendizaje (PEA), conforme a las necesidades que se presentan en el mundo actual. Hoy existe una necesidad imperiosa de ampliar la cobertura y así brindar un mejor servicio de conexión Inalambrica en la red (WiFi) de la Universidad, pero la falta de visión técnica y económica, no ha permitido alcanzar las metas propuestas de implementar una red inalambrica acorde a la tecnología y requerimientos de la UPDS. Con la ampliación de la cobertura mediante acceso inalámbrico, se podrá añadir servicios adicionales a la red universitaria como: acceso constante a Internet, voz IP, videoconferencia, seguridad y autenticación de usuarios. Para lograr el mejor desempeño de todos los procesos académicos en la UPDS, es de vital importancia contar con una red inalámbrica que facilite el acceso a los recursos de la misma y a la vez que se encuentre a la par con la tecnología que cada día se encuentra en un desarrollo constante.

Los procesos informáticos hoy en día, se encuentran muy avanzados a la hora de brindar un servicio de red, ya que brindan la posibilidad de interconectar e interoperar redes o subredes, tanto locales o externas y de incrementar su capacidad de gestión de información. Es por ello que lo que se busca es: "Ampliar la cobertura de la red de la UPDS, para brindar un mejor servicio en todos los procesos informáticos, a la vez mejorar la conexión inalámbrica de la red interna y así poder ofrecer movilidad y conectividad constante, las mismas que darán un mayor valor agregado a la red".

III.1.3. Infraestructura Física de la UPDS

La Universidad Privada Domingo Savio posee una infraestructura física nueva y moderna, debido a que su *campus* universitario fue creado hace 3 años aproximadamente, en octubre del 2008. La óptima educación que brinda a sus estudiantes, mas las evaluaciones constantes a sus docentes, sumadas a la infraestructura física que posee, la califican como una universidad de prestigio en el sur del pais. El *campus* de la Universidad Privada Domingo Savio cuenta con una superficie de 9.004,55 m², con una superficie de construcción de 4.129,83 m^2, que conforman los bloques A, B y la Academia Local Cisco. Existen edificaciones contempladasa futuro y otras que se

encuentran en proceso de creación como ser: la cancha polifuncional (área deportiva).

III.1.3.1. Administración y ubicación de las edificaciones de la UPDS

El estudio de la red de la UPDS, lleva a determinar cómo se encuentran distribuidas, cada una de las edificaciones que conforman las instalaciones del campus universitario.

Bloque A

En el edificio denominado *Bloque A*, se encuentra localizado el auditorio, la sala audiovisual, las fotocopiadoras y las aulas de los estudiantes.

Bloque B

En el edificio denominado *Bloque B,* se encuentran localizados la mayoría de los departamentos administrativos de la universidad, como ser: el Rectorado, Vicerrectorado, Direccion de Gestión Académica, Caja, Registro, etc.; como asi también se encuentran: la biblioteca, soporte técnico y los laboratorios de computación y física-química. El Departamento de Sistemas, que es el encargado del control de la red de la UPDS, se encuentra ubicado en este edificio en el último piso, donde se ubica además el cuarto de telecomunicaciones, donde están los equipos como ser: servidores principales, secundarios, *módems*, *router, switches,* UPS de los equipos, cámaras de vigilancia, etc.

Academia Local Cisco

La academia consta de una sola planta, la que se encuentra dividida en 3 sectores: dos laboratorios y una oficina de información. Además cuenta con su propio sistema de distribución, a la red interna de sus laboratorios mediante un servidor.

III.2. Descripción de la Infraestructura de la Red UPDS[1]

La red interna de la Universidad Privada Domingo Savio (UPDS), está formada por cuatro módems *Zhone* que proporcionan las conexiones de Internet, un *router Cisco 800* y seis *Switches Linksys SR224G,* situados todos en el último piso del *Bloque B*, en el

[1] *Informacion obtenida después de visitar el cuarto de Telecomunicaciones de la UPDS*

cuarto de equipos denominado “Cuarto de Telecomunicaciones”, el mismo que es administrado por el Departamento de Sistemas. Los servidores y demás equipos de administración de la red se distribuyen en el *Rack* existente en el “Cuarto de Telecomunicaciones”, los cuales brindan diferentes servicios y aplicaciones a los usuarios de la Universidad.

El Cuarto de Telecomunicaciones posee un *Rack* vertical, donde se ubican los *switches* principales, los cuales están conectados a través de cableado estructurado a todos los puntos de red existentes en los bloques (A y B) de la universidad y se comunican mediante una conexión WAN a la academia Cisco. En un rack similar, se localizan los equipos de los dos laboratorios con los que cuenta la academia. Toda la distribución de la red se la realiza desde la base principal en el Departamento de Sistemas, que posee equipos para la administración, funcionamiento y el manejo de la red. Dispone de un dispositivo de aire acondicionado, que brinda el ambiente adecuado de trabajo, para los todos los equipos que se encuentran en el Cuarto de Telecomunicaciones, así como regula toda la temperatura, en caso de que se presente algún problema que afecte la refrigeración normal de los elementos de *hardware*. Existen cuatro UPS que almacenan y proveen energía a los dispositivos de administración y control de la red, en caso de ausencia de energía eléctrica.

III.2.1. Situación Actual de la Red WiFi[2]

La red inalambrica actual de la Universidad Privada Domingo Savio, está constituida básicamente por cuatro *routers* de las marcas Cisco y TP-Link, que se distribuyen a un *router* por piso en los bloques A y B, para brindar el servicio de conexión WiFi. La situación actual de la Red Inalambrica de la UPDS, no garantiza una forma eficiente de brindar el mejor servicio de conexión y acceso a la red e Internet, a los usuarios internos (docentes y estudiantes).

Para facilitar la entrada a la nube de Internet, el proveedor de servicios brinda 4 líneas de conexión, es decir cuatro *módems,* uno para cada conexión de Internet que se conecta

[2] *Informacion propocionada por el Departamento de Sistemas de la UPDS*

internamente a la red de la universidad. Como medida de seguridad existe un *firewall* que brinda las seguridades requeridas en la red. El sistema de administración de la red controla de forma global todos los equipos de acceso a la red, existe un *firewall* en software "ISA Server", el cual controla todo el trafico de la red y el acceso a los recursos de la misma.

La red inalambrica de la UPDS posee un *router* TP-Link *TL-WR1043ND* con 3 antenas externas, ubicadas en el primer piso del *Bloque A,* frente a las gradas que conducen al segundo piso. Para los demás pisos, se cuenta con 3 *routers Linksys WRT160N* con antenas internas. El primero ubicado en el tercer piso del *Bloque B*, dentro de la biblioteca, el segundo también ubicado en el tercer piso, cerca de la intersección de los *Bloques A y B* y el tercero, ubicado en el cuarto piso cerca de las intersecciones de los *Bloques A y B.*

Figura III.2 Router TP-Link 1° Piso

Figura III.3 Router Linksys 2° Piso

Figura III.4 Router Linksys 3° Piso

Figura III.5 Router Linksys 4° Piso

Todos los *routers* mencionados, proporcionan conexión a sus respectivos pisos, pero un aspecto importante a tomar en cuenta es, que todos estos *routers* son de bajo rendimiento y corto alcance, debido a la cantidad de interferencias que existen en los ambientes de cada piso. Al ser *routers* diseñados para casas u oficinas, demuestran no ser apropiados para brindar una óptima conexión y brindar los diferentes servicios de la red de la universidad, por tales razones, se llega a la conclusión que la universidad cuenta con un servicio de WiFi bastante pobre.

La Figura III.6 representa el esquema actual de la situación de la red WiFi de la Universidad Privada Domingo Savio.

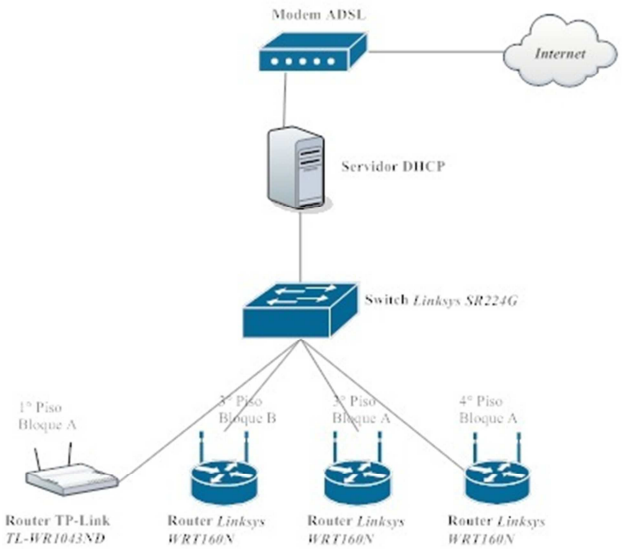

Figura III.6 Diagrama de la Red WiFi Actual de la UPDS

III.2.2. Servicios de la Red

La Universidad Privada Domingo Savio, brinda los servicios actuales como: correo electrónico, Internet y acceso a la base de datos. Mediante este proyecto, se intenta mejorar la red interna y tiene como objetivo, incrementar nuevos servicios a brindar y administrarlos de una forma centralizada y más solvente para cada usuario, como por ejemplo: incluir servicios como VoIP y Videoconferencia.

III.2.2.1. Internet[3]

El proveedor de servicios de Internet con el que actualmente cuenta la Universidad Privada Domingo Savio, es la Empresa Nacional de Telecomunicaciones (ENTEL), la misma que provee cuatro enlaces para toda la Red UPDS, como se describe a continuación:

- 2 Mb para el sector administrativo

[3] *Informacion propocionada por el Encargado del Departamento de Sistemas de la UPDS*

- 2 Mb para el servicio WiFi y la academia Cisco
- 1 Mb para los laboratorios C y D
- 512 Kb para los laboratorios A y B

Se debe tener en cuenta que la capacidad del enlace que brinda ENTEL, es insuficiente para los servicios y aplicaciones que tiene la Universidad, debido a que el ancho de banda distribuido a cada usuario es baja, esto se debe a que se ha estado incrementando el número de usuarios en la red considerablemente y no existen normas o políticas de control y de acceso a la red.

III.2.2.2. Correo Electrónico

El servicio de correo electrónico con que cuenta la Universidad Priv. Domingo Savio, es el *Exchange Server 2003*, ubicado en un servidor independiente; el cual es de uso solo para los docentes y los administrativos, que brinda una cuenta de correo a cada usuario que necesite disponer de este servicio.

III.2.2.3. Base de Datos

La base de datos utiliza un servidor de grandes capacidades de almacenamiento en su disco duro, por el hecho de que es un sistema muy importante en el desarrollo de las aplicaciones de tipo interno, es así que utiliza *SQL Server 2005* bajo sistema operativo Windows. Este sistema utiliza la base de datos para permitir el desarrollo de aplicaciones como: el sistema académico, la web de la universidad, etc, cada uno de los cuales está realizado con lenguaje Java.

III.2.3. Falencias que posee la Red de la UPDS

Al ser una red que no tuvo ningún estudio y análisis previo para su diseño y fue implementada de manera rápida sin una planificación de la misma, puede tener varios problemas a la hora de brindar servicios y satisfacer las necesidades de cada uno de los usuarios de la red. Estos problemas pueden ser de: administración, físicos o técnicos y

hasta a veces de falta de disponibilidad.

Los enlaces inalámbricos entre los bloques del campus universitario, fueron realizados sin ninguna planificación previa, para poder prever su: escalabilidad, cobertura, número de usuarios, etc. Sin embargo estos enlaces tienen un desempeño regular, que permiten la comunicación con la red principal de la UPDS. La asignación de ancho de banda brindado por el proveedor actual, es muy bajo con respecto a lo que se requiere en cada una de las aplicaciones y de acuerdo al número de usuarios existentes.

La red requiere de la elaboración de un documento, que represente el diseño actual de la red, para poder determinar posibles fallas o realizar correcciones. Se necesita de un dispositivo tipo *hardware* ó *software,* que permita el monitoreo y administración de una forma centralizada de toda la red, para así poder determinar y corregir los fallos o la congestión de la red, en cualquier lugar que se produzcan.

Para poder mejorar el servicio de WiFi y ampliar la cobertura de la red, se deberá realizar un estudio y una planificación para el despliegue de nuevos dispositivos inalámbricos y su respectiva ubicación e interconectividad entre los mismos.

CAPITULO IV
DISEÑO DE LA RED INALAMBRICA MESH

CAPITULO IV

Diseño de la Red Inalambrica Mesh

IV.1. Observaciones de Diseño de la red WMN

La propuesta de diseño de una Red Inalámbrica, que provea de servicios de red e Internet a usuarios finales dentro de un campus universitario, debe tomar en cuenta ciertas consideraciones, las mismas que servirán para desarrollar la red *Mesh.* El diseño a ser implementado, debe satisfacer todas las expectativas y necesidades, para lograr un correcto desenvolvimiento y planificación de la red, permitiendo así cumplir con la prestación de servicios, con calidad y seguridad ante el usuario. Existen algunas consideraciones que se debe tener en cuenta, a la hora de conformar un esquema de implementación de una WMN:

- Calidad de Servicio
- Escalabilidad
- Seguridad
- Disponibilidad de Ancho de Banda
- Tipo de aplicaciones
- Administración Centralizada
- Redundancia
- Movilidad
- Rendimiento

IV.2. Descripción de la Tecnología a emplearse en el diseño de la red WMN

La propuesta tecnológica de las redes inalámbricas *Mesh,* es pasar a tener redes *Wireless,* en donde cada nodo sería como una especie de cliente-emisor/repetidor de la red WiFi. Cada nodo se encuentra interconectado con los otros que estructuran la malla vía radio y cada nodo dentro de la red *Mesh*, es capaz de tomar decisiones de trazado de rutas, independiente de los demás nodos, de ahí que en una red inalámbrica *Mesh,* cada

punto de conexión es un "nodo inteligente" interconectado. El establecimiento del estándar 802.11s, permitirá la compatibilidad con los estándares existentes actualmente (802.11a/b/g/n) y además, la interoperabilidad con cualquier fabricante de equipos WiFi para redes *Mesh*. Para el presente diseño se optará por utilizar una red *Mesh* basada en el estándar 802.11a y g/n, ya que presenta mayores ventajas y permitirá migrar al estándar 802.11s, cuando se encuentre totalmente terminado, con todas las características descritas en el Capítulo II. Los equipos y dispositivos trabajarán en la banda de frecuencia de 2.4 GHz y 5 GHz, motivo por el cual:

- No se necesita licencia para el uso del espectro radioeléctrico.
- Se integra rápidamente a las redes cableadas existentes.
- Existe gran variedad de equipos en el mercado.
- Su costo para instalación es mucho menor.
- El estándar 802.11g/n es compatible hacia atrás con el estándar 802.11b.
- El estándar 802.11a es prácticamente libre de interferencias.
- Tanto el estándar 802.11a, b, g y n permiten los enlaces de comunicación de los usuarios finales.

IV.3. Modelo Jerárquico para la red WMN

El diseño de la red *Mesh* dentro del campus universitario, se describirá de acuerdo a un modelo de niveles de jerarquía definidos mediante la Figura IV.1. Cada nivel describe las características de comportamiento presentes en el diseño y divide a la red *Mesh,* donde estarán los encargados de transformar o poder configurarla, para permitir la: escalabilidad, redundancia, incremento de usuarios en la red, fácil detección de errores y la adaptación a cambios tecnológicos

IV.3.1. Nivel 1

Este nivel ofrecerá una conexión lo más rápida posible entre los puntos de distribución y

consta de un *router* principal, el mismo que provee la conectividad entre el exterior y la red interna *Mesh.*

IV.3.2. Nivel 2

El tráfico en la red es dirigido a través de cada uno de los servicios, mediante un *Router*, él mismo que permite alternativas de poder segmentar los dominios de colisión y *broadcast,* para procurar evitar las congestiones en la red principal. Posee dos *switches* de *distribución,* que serán los que manejen todo el tráfico y las políticas de seguridad de la red *Mesh*, los mismos que se conectarán al *router* principal. Además maneja un control al borde de la red con servicios de red inteligentes, incluye calidad de servicio (QoS), clasificación y priorización de tráfico mediante la creación de VLANs.

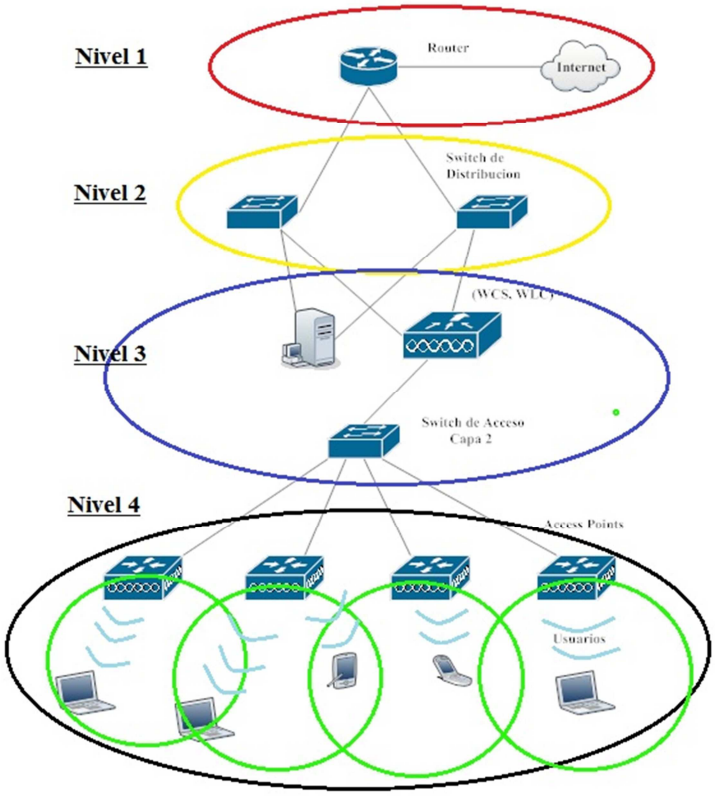

Figura IV.1 Diseño Jerárquico

IV.3.3. Nivel 3

Este nivel permite la administración y sirve como punto de concentración para acceder a cada unos de los servicios de la red *Mesh*. El *switch* maneja una conmutación de paquetes a nivel de capa 2 del modelo OSI. La administración de los recursos de radio frecuencia de todos los *Access Point* (AP) conectados, se la realiza a través del *Wireless LAN Controller* (WLC).

El Wireless Control System (WCS), es una plataforma que permite direccionar la planificación LAN *Wireless*, configuración, administración y movilidad de servicios. Provee un recurso poderoso que permite que el administrador: diseñe, controle y monitoree las redes *Wireless* desde una ubicación centralizada, simplificando las operaciones. El WCS es un componente de *Cisco Unified Wireless Network* que que se explicará mas adelante.

IV.3.4. Nivel 4

Es la capa de acceso de los usuarios a los distintos servicios ofrecidos por la red, la cual se encarga de distribuir los diferentes enlaces inalámbricos hasta el nivel del usuario. Aquí se encuentran ubicados los *Access Point* con sus respectivas configuraciones, dependiendo de la capacidad del número de usuarios finales y la cobertura de cada celda emitida por el *Access Point*. Los dispositivos finales de comunicación, se encuentran accediendo a cada aplicación de red, a través de los *Access Point*, ya que corresponden a la arquitectura de la red inalámbrica *Mesh* de la UPDS. Estos pueden ser equipos portátiles o de escritorio, así como dispositivos WiFi, posteriormente.

IV.4. Calidad de Servicio (QoS)

El uso de las redes inalámbricas está en continua expansión en la actualidad, lo que provoca que cada vez se requiera en ellas “mayor calidad de servicio (QoS)”, a la hora de usarse para aplicaciones en tiempo real. Dado el alto t*hroughput* de las redes *Ethernet,* éstas no han presentado deficiencias en cuanto a calidad de servicio. En cambio, en las redes inalámbricas se requiere de un estándar que garantice QoS en las

aplicaciones en tiempo real, para mejorar la efectividad del uso de estas redes. La calidad de servicio, permite evitar situaciones de congestión en los nodos de la red, proporciona mecanismos para clasificar el tráfico, asigna prioridades en función de cada tráfico, entre otros.

Para poder proporcionar calidad de servicio el 802.11e, usa distintas colas en función del tipo de tráfico. Cada categoría de acceso corresponde a una prioridad y cada una de estas colas, tiene sus propios parámetros de contención y su propio mecanismo de *backoff*. Cada estación 802.11e tiene cuatro categorías de tráfico, se podría dar el caso de que en una misma estación, dos o más colas terminaran el proceso de *backoff* al mismo tiempo, en este caso para evitar el conflicto, transmitiría la de mayor prioridad y el resto se comportarían como si hubiera habido una colisión en el medio. Además existe WiFi Multimedia (WMM), el mismo que es una reformulación de los 8 niveles de prioridad originales de IEEE 802.11e, agrupados en 4 "categorías de acceso". De esta forma el tráfico que se recibe clasificado en el AP, desde la red cableada utilizando IEEE 802.1p ó DSCP, puede ser remarcado en IEEE 802.11, de modo que reciba diferente tratamiento sobre el medio inalámbrico, aumentando la probabilidad de que sea rápidamente transmitido el tráfico de alta prioridad.

El WMM introduce la priorización de tráfico, basándose en la definición de 4 categorías de acceso: platino, oro, plata y bronce. Cuanta más alta es la prioridad, mayor es la probabilidad de que el tráfico sea transmitido en primer lugar. De esta manera, el tráfico de clase platino será enviado antes que el oro, la plata o el bronce. Estas cuatro categorías, pueden mapearse a la marcación que se realiza utilizando DSCP u 802.1p, para facilitar la interoperabilidad de los mecanismos de calidad de servicio, implementados en la red. WMM mapea las prioridades de las 4 colas de transmisión, con los ocho valores de niveles de prioridad que define IEEE 802.11e, de acuerdo a la siguiente lista:

- Voz – Platino: prioridades 6 o 7 de IEEE 802.11e.

- Video – Oro: prioridades 4 o 5.
- *Background* – Plata: prioridades 1 o 2.
- Mejor esfuerzo – Bronce: prioridades 0 o 3.

La mayor parte de los dispositivos *Wireless* de primera marca, disponibles en el mercado actual, implementan WMM y por lo tanto permiten garantizar calidad de servicio en la red inalámbrica.

Para poder implementar el diseño *Mesh* Inalámbrico con QoS (Calidad de Servicio), los equipos que serán utilizados deberán cumplir las siguientes condiciones:

1) Los Access Points, deben estar certificados para QoS y además deben tener esta función activada.

2) Los clientes también deben tener activada la opción de QoS y estar certificados al respecto.

3) Las aplicaciones deben soportar QoS y deben saber asignar los niveles de prioridades, que permite el estándar 802.11e al tráfico que ellas generan.

IV.5. Requerimientos de Ancho de Banda de la red WMN

Se detalla el tipo de aplicaciones y servicios que se usarán, para poder determinar el consumo del ancho de banda y la capacidad de datos; este consumo varía dependiendo de las aplicaciones que cada usuario utiliza. El rendimiento también se lo denomina capacidad del canal**,** o simplemente ancho de banda. El rendimiento de la red de la UPDS será medida de acuerdo a como se encuentren utilizando los recursos cada uno de los usuarios que la conforman, es así que como "no se conoce antecedentes del comportamiento de la red" se realizará un análisis del manejo de la misma mediante conceptos similares usados en otros estudios.

IV.5.1. Requirimientos de Tráfico para cada Aplicación[4]

Para realizar la estimación de tráfico que utilizará cada aplicación dentro de la red, se realizará un estudio estadístico del uso de cada aplicación, debido a que no existen datos anteriores.

IV.5.1.1. Correo Electrónico

Un archivo de correo electrónico promedio se define entre 500 Kbytes, el cual puede contener información como gráficos, texto e información de los usuarios de poco tamaño. Se estima que cada usuario revisa un promedio de 5 correos en 1 hora, con lo que se puede determinar la capacidad que esta aplicación utiliza en la red.

$$\text{Correo} = \frac{500kbytes}{correo} \times \frac{8bits}{1byte} \times \frac{5correos}{60min} \times \frac{1min}{60seg} = 5{,}55kbps$$

IV.5.1.2. Acceso a Internet

Una página Web promedio es de 50 Kbytes, consta básicamente de texto y gráficos de tamaño medianamente normal, un usuario puede acceder a una página Web en 20 segundos, ya que se utilizará un enlace de Internet de banda ancha.

$$\text{Internet} = \frac{50kbytes}{1pagina} \times \frac{8bits}{1byte} \times \frac{1pagina}{30seg} = 13{,}33\text{kbps}$$

IV.5.1.3. Voz Sobre IP[5] (VoIP)

Para aplicaciones que manejan VoIP se considerará para transmisiones aceptables la capacidad de 78.4 Kbps por cada usuario, haciendo referencia al uso del códec G.728, debido a que el tráfico de voz no es tolerante al retardo.

IV.5.1.4. Video Conferencia

Los servicios de videoconferencia y video bajo demanda requieren una capacidad que depende de la calidad de servicio que se ofrecerá. Para una aceptable calidad para

[4] *Datos tomados de la tesis "Diseño de un WISP en el campus de la Universidad Técnica del Norte para proveer servicios de internet inalámbrico utilizando un esquema Wireless Mesh con tecnología Wi-Fi".*
[5] *http://www.voztele.com/esp/productos_servicios_voip/telefonia_ip/telefonia_ip/calidad-QoS-telefonia-ip.htm*

ofrecer videoconferencia permite al menos 15 fotogramas por segundo (15 fps) y capacidades entre 256 y 512 Kbps.

IV.5.1.2. Determinación de ancho de banda necesario para cada servicio

IV.5.1.2.1. Estudiantes

De acuerdo a los resultados obtenidos en una encuesta realizada, se determina el porcentaje de utilización para cada servicio dentro de Internet, estos resultados son mostrados en la Figura IV.2.

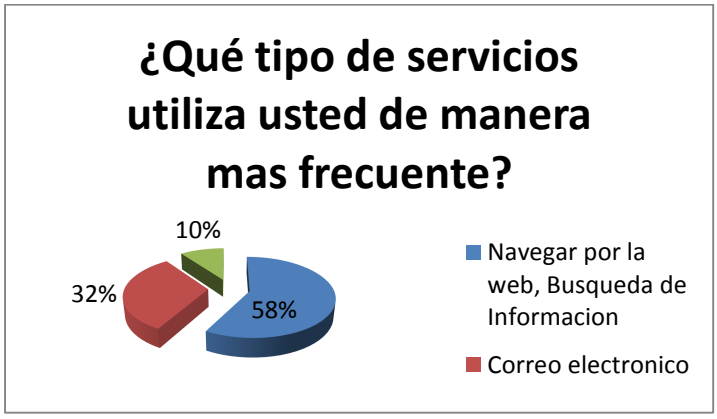

Figura IV.2 Servicios Estudiantes

Estos resultados serán nuestra base para estimar el ancho de banda total que debe tener la red WMN.Otro dato importante es saber el número de usuarios potenciales que estarán conectados a la red para lo cual utilizamos la siguiente tabla, la cual indica el número de estudiantes por facultad de la UPDS del modulo del mes de Marzo del 2012, estos datos fueron obtenidos por el Departamento de Sistemas.

Facultad	**Total Estudiantes**
Ciencias Empresariales	1023
Ciencias y Tecnologias de la Informacion	1135
Humanidades y Ciencias Sociales	586
Total	2744

Tabla IV.1 Cantidad de Estudiantes

De acuerdo a la encuesta realizara se determino que el 58% de los estudiantes cuentan con un dispositivo con conexión WiFi como se muestra en la siguiente grafica:

Figura IV.3 Dispositivos WiFi

De donde podemos decir que del total, hay 1592 estudiantes que cuentan con un dispositivo que les permita conectarse a la red WiFi de la universidad, de esta forma también se pudo determinar que de los 1592 estudiantes con un dispositivo portátil solo el 53% hacen uso de la red WiFi que tiene actualmente la universidad. A continuación se muestra una grafica que representa esta información:

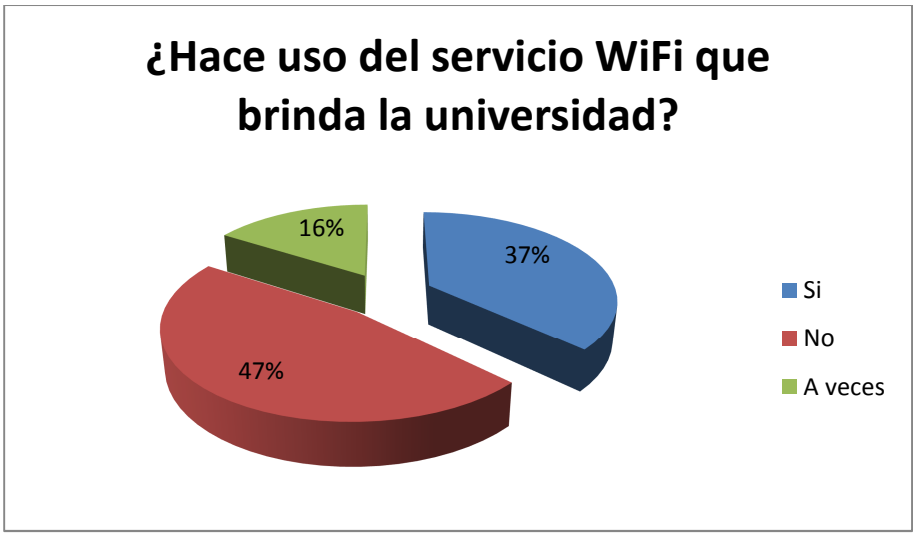

Figura IV.4 Frecuencia de uso WiFi

Entonces determinamos que la red en el caso más crítico (casi nunca se da) tendrá que soportar el tráfico de 844 usuarios al mismo tiempo.

IV.5.1.2.1.1. Correo electrónico

De forma general se determinó que el ancho de banda necesario para este tipo de servicio es 5.55kbps, y de acuerdo a la Figura IV.2 se tiene que el 32% de los encuestados usan correo electrónico, por lo tanto se tiene:

$$\text{Correo} = 5{,}55\text{kbps} \times 0{,}32 \times 844 = 1498{,}944 \text{ kbps}$$

IV.5.1.2.1.2. Acceso a Internet (búsqueda de información)

De forma general se determinó que el ancho de banda necesario para este tipo de servicio es 13.33kbps, y de acuerdo a la Figura IV.2 se tiene que el 58% de los encuestados usan correo electrónico, por lo tanto se tiene:

$$\text{Internet} = 13{,}33 \times 0{,}58 \times 844 = 6525{,}30\text{kbps}$$

IV.5.1.2.1.3. Ancho de banda necesario para aplicaciones adicionales

Para el cálculo del ancho de banda adicional, se considera las descargas como servicio adicional, dejando para el futuro crecimiento de la red los servicios de voz y videos. Entonces el ancho de banda determinado para las descargas será de 1Mbps.

IV.5.1.2.1.4. Capacidad total

La capacidad total para brindar servicio de internet a la UPDS, se obtiene sumando los valores calculados de los diferentes servicios que prestara el diseño de la red WMN. No se considera los servicios de voz y video, ya que en la actualidad estos servicios no son utilizados, pero eso no quiere decir que en el futuro este tipo de servicio no sea necesario.

Capacidad total = 1498,944 kbps + 6525,30kbps + 1000 kbps = 9024,244 = 9Mbps

IV.5.1.2.2. Docentes

De acuerdo a los resultados obtenidos en una encuesta realizada, se determina el porcentaje de utilización para cada servicio dentro de Internet, estos resultados son mostrados en la Figura IV.5.

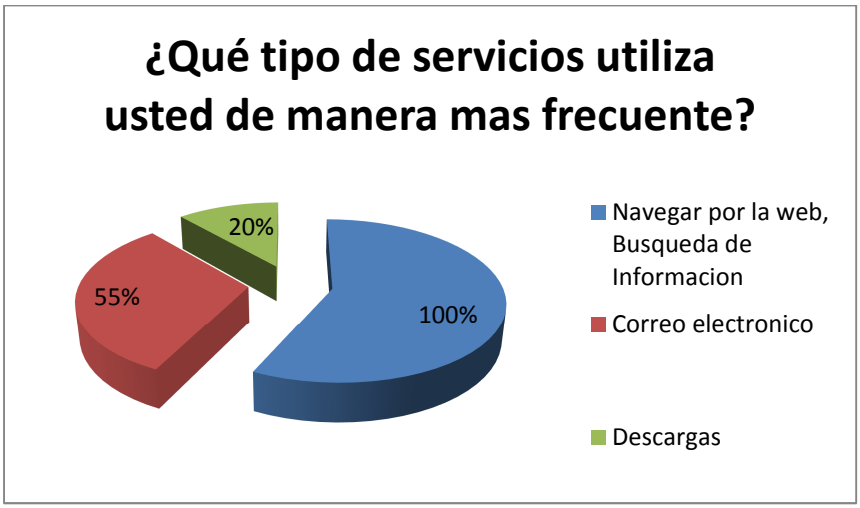

Figura IV.5 Servicios Docentes

Estos resultados serán nuestra base para estimar el ancho de banda total que debe tener la red WMN.Otro dato importante es saber el número de usuarios potenciales que estarán conectados a la red para lo cual utilizamos la siguiente tabla, la cual indica el número de docentes por facultad de la UPDS del modulo del mes de Marzo del 2012, estos datos fueron obtenidos por el Departamento de Sistemas.

Facultad	**Total Docentes**
Ciencias Empresariales	31
Ciencias y Tecnologias de la Informacion	34
Humanidades y Ciencias Sociales	17
Total	82

Tabla IV.2 Cantidad de Docentes

De acuerdo a la encuesta realizara se determino que el 74% de los docentes cuentan con un dispositivo con conexión WiFi como se muestra en la siguiente grafica:

Figura IV.6 WiFi Docentes

De donde podemos decir que del total, hay 61 docentes que cuentan con un dispositivo que les permita conectarse a la red WiFi de la universidad, de esta forma también se pudo determinar que de los 61 docentes con un dispositivo portátil solo el 77% hacen uso de la red WiFi que tiene actualmente la universidad. A continuación se muestra una grafica que representa esta información:

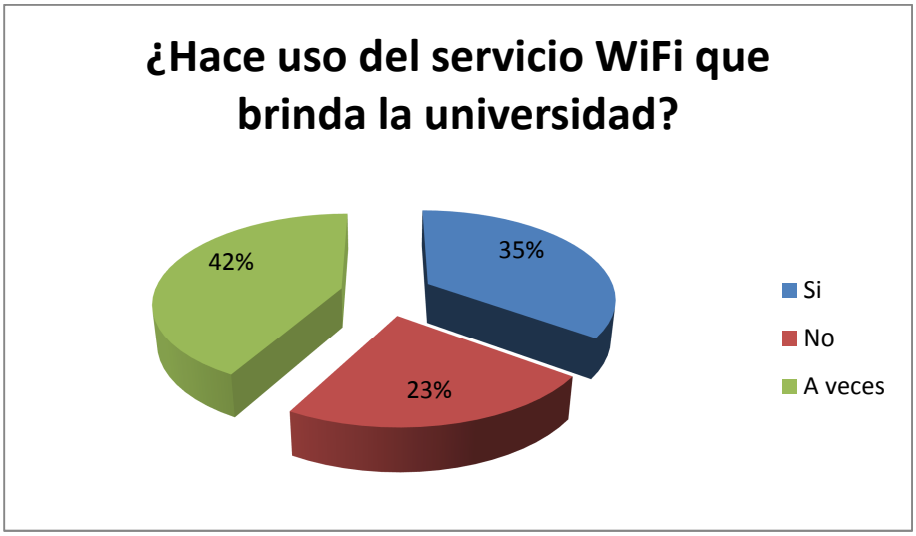

Figura IV.7 Uso de WiFi Docentes

Entonces determinamos que la red en el caso más crítico (casi nunca se da) tendrá que soportar el tráfico de 47 usuarios al mismo tiempo.

IV.5.1.2.2.1. Correo electrónico

De forma general se determinó que el ancho de banda necesario para este tipo de servicio es 5.55kbps, y de acuerdo a la Figura IV.5 se tiene que el 55% de los encuestados usan correo electrónico, por lo tanto se tiene:

$$\text{Correo} = 5{,}55\text{kbps} \times 0{,}55 \times 47 = 143{,}46 \text{ kbps}$$

IV.5.1.2.2.2. Acceso a Internet (búsqueda de información)

De forma general se determinó que el ancho de banda necesario para este tipo de servicio es 13.33kbps, y de acuerdo a la Figura IV.5 se tiene que el 100% de los encuestados usan correo electrónico, por lo tanto se tiene:

$$\text{Internet} = 13{,}33 \times 1 \times 47 = 626{,}51\text{kbps}$$

IV.5.1.2.2.3. Ancho de banda necesario para aplicaciones adicionales

Para el cálculo del ancho de banda adicional, se considera las descargas como servicio adicional, dejando para el futuro crecimiento de la red los servicios de voz y videos. Entonces el ancho de banda determinado para las descargas será de 1Mbps.

IV.5.1.2.2.4. Capacidad total

La capacidad total para brindar servicio de internet a la UPDS, se obtiene sumando los valores calculados de los diferentes servicios que prestara el diseño de la red WMN. No se considera los servicios de voz y video, ya que en la actualidad estos servicios no son utilizados, pero eso no quiere decir que en el futuro este tipo de servicio no sea necesario.

Capacidad total = 143,46 kbps + 626,51kbps + 1000 kbps = 1769,97 = 1,8 Mbps

IV.6. Características de las redes WMN de Cisco

IV.6.1. Características Generales

IV.6.1.1. La creación de redes Mesh permite una implementación rentable de redes WiFi en una ciudad o campus

Una red inalambrica *Mesh* de Cisco, elimina la necesidad de un *Access Point* para conectarse a su propia LAN cableada. En cambio, los *Access Points* en una red *Mesh,* se descubren mutuamente de forma automática y eligen el mejor camino para maximizar las capacidades del sistema y minimizar la latencia. Si un enlace se degrada, el *Access Point* determina si existe un mejor camino y redirige el tráfico a la misma. La solución de la red inalámbrica *Mesh* de Cisco, esta basada en nuevos protocolos de enrutamiento y:

- Hace que sea más fácil y rentable ampliar el alcance de una red inalámbrica para grandes recintos.
- Es fácil de conectar a una red cableada o inalambrica existente, para que así los usuarios puedan desplazarse de un lugar a otro sin la necesidad de reconectarse.
- Permite a los administradores establecer una política de acceso, que funciona en todos los ambientes, aumentando la seguridad y haciendo la infraestructura de la red de todo el sistema más manejable.

IV.6.1.2. Amplia demanda de acceso inalámbrico

Hotspots WiFi autónomos*,* pueden proporcionar capacidad suficiente para una amplia cobertura, pero sin la tecnología *Mesh,* puede ser difícil y costoso ampliar el alcance de la cobertura mas allá de un *hotspot.* En cuanto a las redes celulares, no pueden utilizarse para proporcionar servicios de datos compartidos a cientos o miles de usuarios y son caros para tenerlos y operarlos.

Mientras tanto, según ***Gartner Research*****:** "La creación de redes *Mesh* en varias aplicaciones, se esta convirtiendo en una alternativa de bajo costo para los municipios. Ciudades y pueblos, deberían evaluar las tecnologías *Mesh* para mejorar las comunicaciones de datos y mejorar la interoperabilidad de seguridad pública. Detrás de

tales desarrollos existen ganancias de productividad, facilidad de desarrollo y la capacidad de entregar interoperabilidad *first-responder,* a una fracción de costo de un sistema de radio móvil de tierra.”

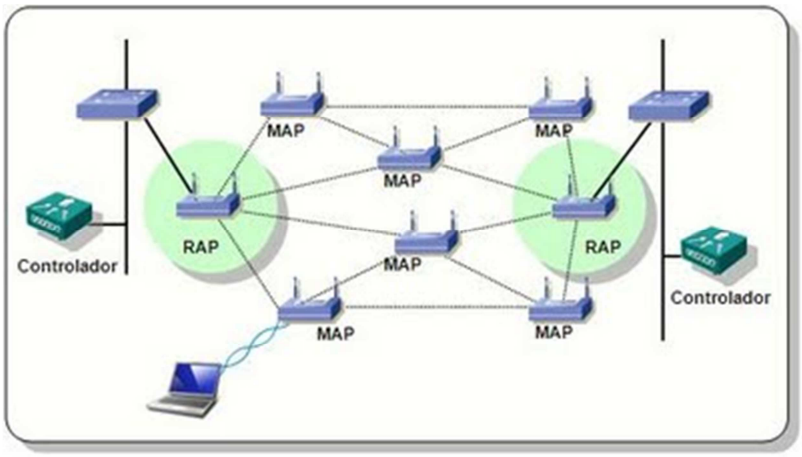

Figura IV.8 Diagrama de una Red Mesh Cisco

IV.6.1.3. Capacidades técnicas

La solución de “Red Inalámbrica *Mesh* de Cisco”, esta basada en la serie de *Cisco Aironet* 1500, un *Access Point* de la red WiFi *Mesh* (802.11/a/b/g), diseñado específicamente para la cobertura segura de exteriores, usando una patente en trámite del protocolo AWPP (Adaptive Wireless Path Protocol). Ofrece las siguientes capacidades:

Facilidad de implementación: Sin configuración de implementación, permite añadir nuevos *Access Points* sin necesidad de configurarlos en el sitio. Ofrece multiples opciones de energía, incluyendo *Power Over Ethernet* (PoE) y opciones de montaje vertical u horizontal en postes.

Capacidad de administración: La red *Mesh* puede estar integrada con una red cableada Cisco existente, permitiendo una configuración central y una gestión de políticas idénticas. Las redes *Mesh* de Cisco, también pueden auto-curarse después de interferencias o interrupciones.

Escalabilidad: La arquitectura hace que sea fácil de escalar la cobertura, permitiendo aumentar la densidad o cantidad de *Access Points*, añadir conexiones cableadas,

controladoras y usa doble alta-potencia y radios de gran sensibilidad, con una selección de antenas de gran ganancia.

Seguridad: La seguridad multi-capa se basa en el IEEE 802.11i, encriptación AES en enlaces de *backhaul*, autenticación de *Access Points*, control de tráfico entre el *Access Point* y la controladora y IPSec VPN para confidencialidad del trafico de clientes Mesh. Los administradores pueden crear políticas de seguridad para los diferentes tipos de usuarios o trafico basado en localización.

Fiabilidad: Recintos resistentes que protegen contra el clima y la vibración de las tormentas o el tráfico saturado. La red dispone de auto-curacion, balanceo de carga automatico entre las controladoras de la WLAN y el canal o la reasignación de la controladora en caso de conflictos.

***Rendimiento*:** Una red *Mesh* de Cisco, ofrece un alto rendimiento mediante la optimización de rutas dinámicas, cuando nuevos sectores son añadidos, además resistencia y mitigación de interferencias.

Flexibilidad: Los *Access Points* que disponen, son dual-band con soporte simultáneo para IEEE 802.11a/b/g y soporte de hardware para la frecuencia segura 4,9 GHz. Soporte de multiples WLAN, permitiendo a los multiples servicios que se ofrecerán a diferentes tipos de usuarios, sobre un único *Access Point.*

Movilidad: Los clientes WiFi tienen movilidad de capa 2 y 3 a través de una red *Mesh*. Los usuarios pueden hacer *roaming* entre *Access Points* en la misma o diferentes controladoras, asi como entre la WLAN Cisco y las redes *Mesh.*

IV.6.2. Características Específicas

IV.6.2.1. Tecnología ClientLink

Muchas redes siguen soportando clientes mixtos 802.11a/g y 802.11n. Debido a que los clientes 802.11a/g operan a bajas velocidades, los clientes antiguos pueden reducir la capacidad de la red. La tecnología ClientLink de Cisco, puede ayudar a resolver los problemas relacionados con la adopción de 802.11n en redes mixtas, asegurando que los clientes 802.11a/g, operen a las mejores velocidades posibles, especialmente cuando estan cerca de los límites de la celda. ClientLink utiliza técnicas avanzadas de

procesamiento de señales y rutas múltiples de transmisión, para optimizar la señal recibida por clientes 802.11a/g en la dirección del enlace descendente, sin necesidad de retroalimentación.

Debido a que no es requerida una especial retroalimentación, Cisco ClientLink funciona con todos los clientes existentes 802.11a/g. La tecnología ClientLink de Cisco permite efectivamente que el *access point* pueda optimizar el SNR, exactamente en la posición donde el cliente se encuentra. ClientLink proporciona una ganancia de casi 4 dB en la dirección del enlace descendente. ClientLink en los *access points* 1552 esta basado en la disponible capacidad ClientLink de los AP 3500s. Por lo tanto, el *access point* tiene la capacidad de *beamform* a los clientes más cercanos y actualizar la información *beamforming* sobre 802.11 ACKs. Incluso si no hay tráfico dedicado de enlace ascendente, ClientLink funciona bien, lo cual es beneficioso para el flujo de tráfico, tanto para TCP y UDP. No hay marcas de agua RSSI, el cual el cliente tiene que cruzar para tomar ventaja del *Beamforming* con los *access points* Cisco 802.11n. Aunque ClientLink se aplica a las porciones existentes de paquetes OFDM, que se refiere a la 11a/g (no 11b) para *access points* 802.11n de interiores y exteriores. Hay una diferencia entre ClientLink 11n de interiores y 11n de exteriores, para *access points* 11n de interiores, el SW limita las tasas de transferencia a 24, 36, 48 y 54 Mbps. Esto se hace para evitar que se junten los clientes a una distancia de un AP en ambiente interiores. El SW también no permite trabajar ClientLink para tasas de transferencia para clientes 11n, debido a que el aumento de rendimiento es mínimo. Sin embargo, hay una ganancia demostrable para los clientes puros. Para *access points* 11n, necesitamos una mayor cobertura, por lo tanto, tres tipos de legado de datos adicionales inferiores a 24 Mbps se han añadido. ClientLink para exteriores es aplicable a tasas de transferencia de 9, 12, 18, 24, 36, 48 y 54 Mbps.

IV.6.2.2. Tecnologia CleanAir

La serie 1550 utiliza la tecnología 802.11n, con radio integrada y antenas internas/externas. La serie 1550 de *access points* estan basados en el mismo *chipset*

CleanAir del AP Aironet 3500. En otras palabras, los *access points* 1550 son capaces de hacer CleanAir. CleanAir en *Mesh* (1552 y 3500) puede ser implementado en el radio 2,4 GHz y proporciona clientes 802.11n, mientras estan detectando, localizando, clasificando y mitigando las interferencias de RF.

Esto proporciona una administracion de clase portadora y la experiencia del cliente y asegura el control sobre el espectro en la ubicación de implementacion. CleanAir permite la tecnología RRM en la plataforma exterior 11n, cuantifica, y mitiga interferencias WiFi y no-WiFi en radios 2.4 GHz. AP1552 soporta CleanAir en 2.4 GHz en clientes en modo de acceso. AP3500 en modo *bridge* (mesh) también soporta CleanAir en 2.4 GHz acceso solo para clientes y no *backhaul.*

IV.6.2.2.1. Modos de funcionamiento CleanAir

IV.6.2.2.1.1. Modo AP Bridge (Mesh) (recomendado)

AP 1552 en modo *bridge* (mesh) ofrece completa funcionalidad CleanAir en la banda 2,4 GHz. Modo *bridge* (mesh) es el modo equivalente a modo local (LMAP) para *access point* CleanAir comunes en cuanto a funcionalidad CleanAir se refiere. AP 1552 viene sólo en el modo *bridge* y el modo no puede ser cambiado. Un *access point Mesh* lleva a cabo la función CleanAir y también presta servicios a clientes en el canal asignado de forma similar a Cisco *Indoor CleanAir* AP 3500 (modo no-mesh) que funciona en modo LMAP atendiendo a clientes en el canal asignado.

El AP *Mesh* también monitorea el espectro sólo en ese canal. La funcionalidad CleanAir similar es aplicable a AP 3500 en modo *Mesh.* Cuando AP 3500 está en modo *no-Mesh*, el AP puede realizar la función CleanAir en LMAP o en modo monitor. Cuando el AP 3500 está en modo *Mesh,* el AP puede realizar la función CleanAir en modo *bridge* (mesh) en 2,4 GHz, atendiendo clientes al mismo tiempo en el canal asignado. La integración de silicio con el radio WiFi, permite al *hardware* CleanAir escuchar entre el tráfico del canal que está siendo usado, sin ninguna sanción para el rendimiento de

clientes conectados, es decir, la detección de la tasa de transferencia sin interrumpir el tráfico del cliente.

AP 1552 en acceso de clientes 2,4 GHz, ofrece *Radio Resource Management* (RRM), que ayuda a mitigar la interferencia de fuentes de interferencia WiFi. RRM no está disponible en 5 GHz *backhaul*. Un AP *Mesh* CleanAir, sólo analiza un canal de cada banda continuamente. En una normal implementaacion de alta densidad, debe haber muchos *access points* en el mismo canal y al menos una en cada canal, suponiendo que RRM se encarga de la selección de canales.

En 2,4 GHz, los *access points* tienen una densidad suficiente para asegurar por lo menos tres puntos de clasificación. Una fuente de interferencia que utiliza la modulación de banda estrecha (opera alrededor de una sola frecuencia), sólo es detectada por *access points* que comparten el espacio de frecuencia. Si la interferencia es un tipo de salto de frecuencia (usa múltiples frecuencias, generalmente, cubriendo la toda la banda), es detectada por cada *access point* que puede escuchar la operación en la banda.

IV.6.2.2.1.2. Modo Monitor AP (MMAP) (opcional)

Un AP CleanAir en modo monitor es dedicado y no brinda tráfico de cliente. El modo monitor asegura, que todas las bandas y canales son rutinariamente escaneadas. El modo monitor no está disponible para AP 1552 y 3500 en modo *bridge* (mesh), porque en un entorno *Mesh*, los *access points* también hablan el uno con el otro mediante *backhaul.* Si un AP *Mesh* (MAP) está en el modo monitor, entonces no puede realizar operaciones *Mesh*. Además, no es posible para AP 1552 o AP 3500 (modo bridge) estar en modo monitor dedicado.

IV.6.2.2.1.3. Spectrum Expert Mode Connect (SE Connect) (opcional)

SE Connect AP, es configurado como un sensor de espectro dedicado, que permite la conexión de la aplicación Cisco Spectrum Expert, que se ejecuta en un *host* local para utilizar AP CleanAir, como un sensor remoto para el espectro de la aplicación local. Este

modo permite la visualización de los datos del espectro tales como: tramas FFT y mediciones más detalladas. Este modo esta destinado únicamente para solución remota de problemas.

IV.7. Planificación de la Red WMN

La realización de la red inalámbrica, está basada en un esquema *Mesh* (mallado), debido a que estas redes presentan características tales como: redundancia, auto-reparables, tolerantes a fallos, mayor área de cobertura, administración más simple y eficiente, etc. La arquitectura de la red inalámbrica, tiene como objetivo en su implementación, proveer a los usuarios el acceso a la red e Internet, donde cada usuario podrá acceder a este servicio, mediante un equipo portátil independientemente del lugar donde se encuentre, siempre y cuando esté dentro del área de cobertura de la red, para lo cual se utilizará equipos y dispositivos que utilizan tecnología WiFi, pues se pretende cubrir la mayor parte del área del campus universitario. Los *Access Point,* tanto la cantidad, como las características de cada uno, se las realizará mediante una planificación de estudio, asumiendo detalles para el dimensionamiento de los mismos y que sean capaces de satisfacer la demanda de cada usuario estimado, que pretenda utilizar este servicio y se maneje con valores aceptables de eficiencia y confiabilidad, para la seguridad interna de los datos.

El diseño de la red inalámbrica dentro de las instalaciones de la UPDS, no compartirá recursos de la red LAN interna, ya que la disposición de algunos equipos no prestan las condiciones necesarias para estructurar un sistema *HIBRIDO* y por motivos de seguridad el único recurso compartido será el servidor DHCP para brincar direcciones IP a los usuarios que se conecten a la red *Mesh,* dejando el servidor de correos y el servidor de base de datos separados de la red *Mesh*, con acceso solo desde la red cableada. Así mismo se adquirirán los equipos y demás elementos que se necesitaran, para permitir un funcionamiento del sistema, acorde con las expectativas requeridas.

IV.7.1. Diseño de la Red WMN

La propuesta de diseño de la red inalámbrica para la Universidad Privada Domingo Savio, está relacionada con la consolidación de los recursos de: control, administración, seguridad y monitoreo, de los dispositivos que interactúan en la red Inalámbrica *Mesh* de una forma centralizada. Se implementará una solución unificada que brinda Cisco y que permite un mejor desarrollo.

IV.7.1.1. Plataforma Unificada

Una solución unificada de redes inalámbricas, contemplará la integración de: seguridad, administración y operación centralizada, así como el acceso a usuarios dentro de la red inalámbrica. Dicha solución permite correr servicios de video, voz y datos, dentro de una misma plataforma de red. La solución unificada de redes inalámbricas de área local (WLAN), permite el acceso seguro a recursos disponibles, así como acceso a invitados, permitiendo una fácil administración de su infraestructura, mediante la centralización de la operación.

La administración centralizada de redes inalámbricas, reduce sus costos de operación, al tener que asignar menos recursos para su buen funcionamiento. La solución unificada de redes inalámbricas, integra el acceso seguro a la red mediante el método más conveniente, dependiendo de las políticas de seguridad implementadas, así como la proyección de crecimiento. La administración se ve significativamente mejorada, debido a la autoconfiguración de su infraestructura inalámbrica y a la fácil visualización de la red, donde cada operación es realizada desde un solo punto, permitiendo de esta forma reducir costos en recursos asignados con dicho propósito.

IV.7.1.1.1. Beneficios

Dentro de esta alternativa existen algunos beneficios que sustentan la implementación de una solución unificada para redes inalámbricas.

- Administración y Operación Centralizada.

• Seguridad mediante el acceso inalámbrico.
• Localización de dispositivos WiFi en tiempo real.
• Cobertura en áreas exteriores o extensas.
• Una sola plataforma para correr servicios de Datos, Voz y Video.

IV.7.1.1.2. Componentes de la Solución Unificada

Existen algunos componentes que intervienen en la solución unificada de redes inalámbricas de Cisco, los cuales son:

• *Access Point* (AP)
• *Wireless LAN Controller* (WLC*)*
• *Wireless Control System* (WCS)

IV.7.1.1.2.1. Access Point

Los APs hablan *Lightweight Wireless Access Point Protocol (*LWAPP) contra el *Wireless LAN Controller* y éste controla la potencia irradiada y centraliza el tráfico. Las políticas de seguridad y QoS son dirigidas por este controlador central.

IV.7.1.1.2.2. Wireless LAN Controller

El Wireless LAN *Controller,* trabaja en conjunto con el AP, comunicándose con éste por medio de LWAPP, es el responsable de implementar una política centralizada de QoS, seguridad y manejo de RF (Radio Frecuencia). Para escalar en cantidad de APs, se pueden colocar los *Wireless LAN Controllers* en *clúster*. Un *clúster* puede tener como máximo 24 *Wireless LAN Controllers*, brindando un crecimiento en cantidad de APs, todos ellos con una política de QoS, seguridad, uniformes. El *Wireless LAN Controller* agrega inteligencia al manejo de RF, brindando las siguientes funcionalidades:

- Asignación dinámica de los canales sin solapamiento a cada AP.
- Detección de interferencias. El LAN *Controller* detecta interferencias y recalibra los parámetros de RF para evitarlos.

- Balanceo de carga entre APs.
- Detección de zonas sin cobertura; incrementa la potencia de los APs aledaños para cubrir dichas zonas.
- Redundancia N+1. En caso de falla del LAN *Controller*, los APs se mueven al *backup.*
- Se encarga de aplicar las políticas de seguridad 802.1X, EAP, WAP y WEP, con las siguientes características: QoS por asignación de múltiples niveles de servicio, *traffic-shapping* y utilización del medio RF. Seguridad en nivel 2 (802.1X, WEP y WPA). Seguridad en nivel 3 (IPSec y Web Authentication). Encriptación del tráfico entre el *Wireless LAN Controller* y el AP.

IV.7.1.1.2.3. Wireless Control System

El WCS *Wireless Control System,* trabaja en conjunto con el AP y el *Wireless LAN Controller*. El WCS es la herramienta de software que provee medios gráficos para el planeamiento y *troubleshooting* de la infraestructura WiFi. Corre sobre un servidor Linux o Windows y se accede mediante un *Web browser*. Un WCS soporta hasta 1500 APs.

El WCS permite:

- Diseñar la red *Wireless* posicionando los APs geográficamente en un mapa y visualizando la cobertura.
- Visualización en tiempo real de la cobertura WiFi y de parámetros propios de RF (nivel de ruido, SNR, interferencias, nivel de potencia y la topología de la red).
- Detección de ataques de RF del tipo DoS y bloqueo automático del usuario malicioso.
- Detección de APs ajenos y conexiones *ad-hoc.*
- Creación y ampliación de las políticas de seguridad por SSID.
- Soporte de hasta 16 SSID diferentes.

IV.7.2. Cobertura de la Red WMN[6]

El diseño de la red inalámbrica *Mesh,* implementa 17 *Access Points* de interiores (indoor) y 2 *Access Points* de exteriores (outdoor), llegando a satisfacer los requerimientos, para que cada uno de los usuarios pueda acceder sin ningún problema a la red, mediante un enlace inalámbrico. La Figura IV.9 describe las áreas de cobertura de los *Access Points* internos y externos, distribuidos de forma que puedan ser utilizados por el mayor número de usuarios.

Se determinaron las áreas de cobertura y la posición para cada equipo, con *Access Points* Cisco Aironet 1552e, para *outdoor* y 3500p para *indoor*, con antenas omnidireccionales en las frecuencias de 2,4 GHz y 5GHz respectivamente, ya que estos equipos poseen las mejores características para la implementación de la red inalámbrica *Mesh* dentro del campus universitario.

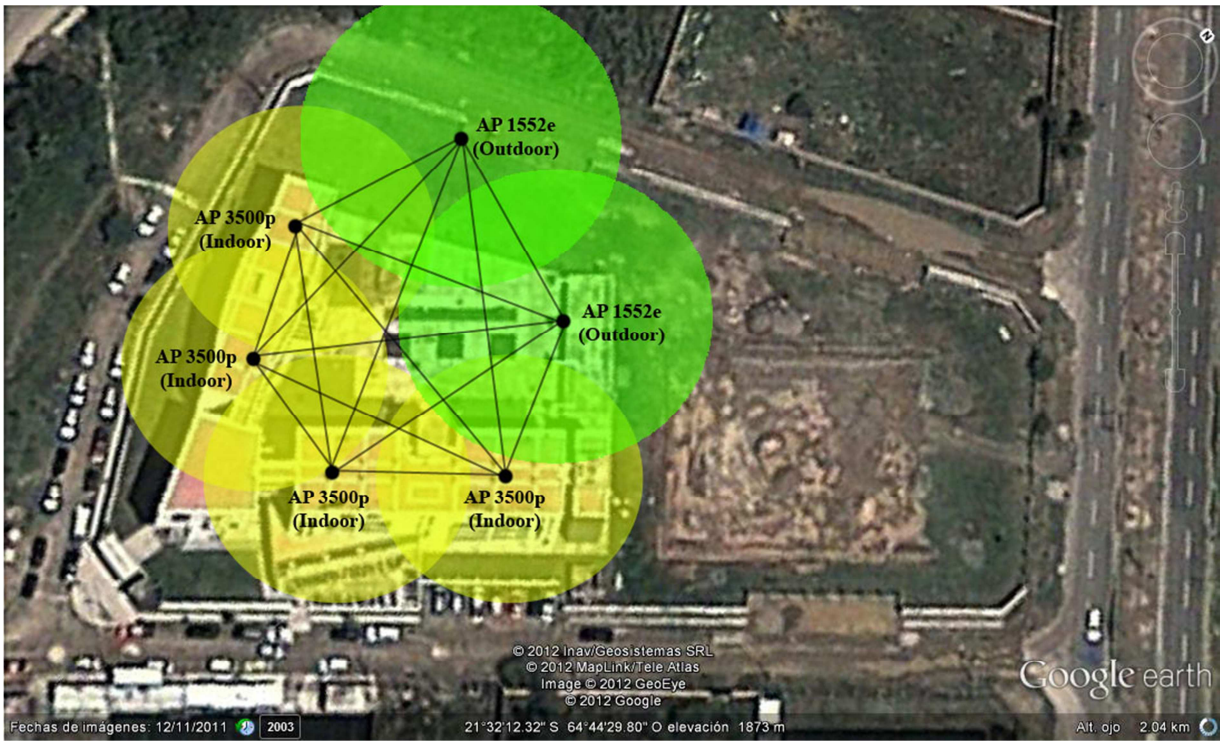

Figura IV.9 Cobertura de la Red WMN

[6] *Ver Anexo A (Reporte generado por el WCS)*

Para el sector de la cancha polifuncional en construcción, se estima que una vez finalizada su construcción, se aumentará un equipo de *outdoor* al diseño de la red, para cubrir la cobertura de esta zona y se determinará que afluencia de personas existirán que demanden conexión a la red e Internet.

IV.7.3. Protocolo de enrutamiento para la Red WMN [79]

IV.7.3.1. Protocolo AWPP (Adaptive Wireless Path Protocol)

Adaptive Wireless Path Protocol (AWPP), es un protocolo propietario de Cisco para redes inalámbricas *Mesh*. Descubre dinámicamente radios vecinos y calcula la calidad de todas las trayectorias posibles a una red cableada. Una trayectoria óptima, se establece a través de una malla de nodos inalámbricos a una puerta de enlace por cable y estos cálculos son continuamente actualizados, permitiendo que las trayectorias cambien y se optimicen, mientras que los patrones de tráfico en enlaces inalámbricos cambian. Además, se crea un *backhaul* inalámbrico, que permite la auto-configuración y auto-curación del enlace. La especificación del enlace inalámbrico y del protocolo del enrutamiento, es definida por el grupo de trabajo 802.11s (TG-S).

IV.7.3.1.1 Prevención de bucles

Para asegurarse de que los *bucles* de enrutamiento no sean creados, AWPP descarta cualquier ruta que contenga su propia dirección MAC. Es decir, la información de enrutamiento, separada desde cada salto de información, contiene la dirección MAC de cada salto al RAP, por lo tanto, un MAP puede detectar fácilmente y desechar rutas que conformen un *bucle.*

IV.7.3.2. Arquitectura

La red de enlaces inalámbricos de Cisco, utiliza un diseño dual-radio que realza el funcionamiento y la confiabilidad del acoplamiento sin hilos. En esta arquitectura, el sistema WLAN del regulador, se utiliza para crear y para hacer cumplir políticas a través de muchos y diversos *Access Points LightWeight.* Usando la calidad de servicio (QoS) y

otras funciones, las operaciones al aire libre de la WLAN, se pueden manejar eficientemente a través de una empresa inalámbrica entera.

IV.7.3.3. Comparación con arquitecturas tradicionales

La arquitectura tradicional, limita la visibilidad del tráfico 802.11 a un *Access Point* individual, puesto que distribuye toda la dirección de tráfico, control de RF, seguridad y funciones de movilidad de los *Access Point.*

IV.7.4. Estándares IEEE 802.11 usados en el diseño de la red WMN

Para la elaboración del diseño de la red *Mesh* para el campus de la UPDS se utilizaron los siguientes estándares WiFi:

Para la transmisión de datos:

- 802.11a
- 802.11b
- 802.11g
- 802.11n

Para la Calidad de Servicio (QoS):

- 802.11e

Para la seguridad:

- 802.11i

Para la tecnología Mesh

- 802.11s

IV.7.5. Especificaciones para la implementación del diseño de la red WMN

A continuación se presentan algunas especificaciones a tomar en cuenta a la hora de hacer la implementación de la red *Mesh.*

IV.7.5.1. Elección de los RAP y MAP

Los puntos de acceso dentro de una red *Mesh*, pueden operar en una de las dos formas siguientes:

1. Root Access Point (RAP)
2. Mesh Access Point (MAP)

Todos los access points son configurados y enviados como access points *Mesh*. Para usar un access point como *root access point*, se debera volver a configurar el access point *Mesh* a un *root access point*. En todas las redes *Mesh*, asegurese que existe al menos un *root access point*.

Mientras que los RAPs tienen conexiones por cable a su controladora, los MAPs tienen conexiones inalámbricas a su controladora. MAP se comunican entre sí y de vuelta al RAP mediante conexiones inalámbricas radio backhaul 802.11a/n. MAPs usan Cisco Adaptive Wireless Path Protocol (AWPP) para determinar la mejor ruta a la controladora a través de otros access points *Mesh*.

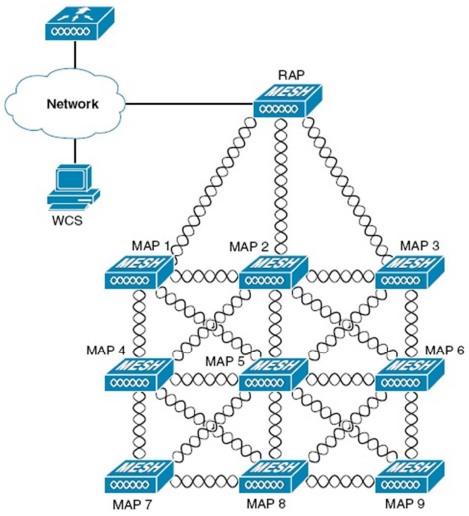

Figura IV.10 Ejemplo de RAP y MAP

IV.7.5.2. Preparación y Planificación del sitio[7]

Esta sección proporciona detalles de implementación.

IV.7.5.2.1. Estudio del Sitio

Recomendamos que realice una inspección de radio del sitio antes de instalar el equipamiento. Un estudio del sitio revela problemas como las interferencias, zona de Fresnel o problemas de logística. Un estudio del sitio propiamente dicho involucra temporalmente el establecimiento de enlaces *Mesh* y permite tomar medidas para determinar si los cálculos de las antenas son exactos. Determina la ubicación y la antena correcta antes de perforar agujeros, realizar el tendido de cables y montar el equipo.

IV.7.5.2.1.1. Estudio del Sitio Exterior

Implementación de sistemas WLAN en exteriores requiere de un conjunto de habilidades diferentes a las instalaciones inalámbricas en interiores.

Consideraciones como las temperaturas extremas, rayos, seguridad física y las regulaciones locales deben ser tomadas en cuenta.

Al determinar la idoneidad de un enlace *Mesh* exitoso, hay que definir hasta qué punto el enlace *Mesh* se espera tener transmision y que velocidad de radio. Recuerde que la velocidad no esta incluida directamente en el calculo del enrutamiento inalámbrico y recomendamos que la misma velocidad sea utiliza a lo largo de la misma malla (la velocidad recomendada es 24 Mbps).

Recomendaciones de diseño para enlaces *Mesh*:

- La implementación de un MAP no puede exceder los 35 pies (10,668m.) de altura sobre la calle.
- Los MAP están implementados con antenas apuntando hacia abajo, hacia el suelo.
- Distancias típicas de 5 GHz entre RAP y MAP son 1000 a 4000 pies. (304,8m a 1219,2m).
- Ubicación de RAP son típicamente torres o edificios altos.

[7] *Ver Anexo B (Vista 3D)*

- Distancias típicas de 5 GHz entre MAP y MAP son de 500 a 1000 pies (152,4m a 304,8m).
- Ubicación de MAP son típicamente edificios cortos y postes de luz.
- Distancias típicas de 2.4 GHz entre MAP y clientes son de 500 a 1000 pies (152,4m a 304,8m) (depende del tipo de *acces point*).
- Los clientes suelen ser ordenadores portátiles, teléfonos inteligentes, tablets y CPEs. La mayoría de los clientes operan en la banda 2,4 GHz.

IV.7.5.2.2. Consideraciones de Cobertura de la red inalambrica Mesh

Esta sección provee un resumen de los elementos que deben ser considerados para una máxima cobertura LAN inalámbrica en una zona urbana o suburbana, para adherirse a las condiciones de cumplimiento para los respectivos dominios. Las siguientes recomendaciones suponen un terreno plano sin obstáculos.

IV.7.5.2.2.1. Planificación de Celda y Distancia

IV.7.5.2.2.1.1. Para la serie 1550

Se recomienda una celda de radio de 600 pies (182,88m), y una distancia entre APs de 1200 pies (365,76m). Normalmente, se recomienda que la distancia entre APs sea el doble de la distancia entre un AP y un cliente. Es decir, si tomamos la mitad de la distancia entre APs, tendremos el radio de la celda aproximado.

La serie 1550 ofrece comparativamente mejor rango y capacidad que tiene la funcionalidad 802.11n. Tiene ventajas de ClientLink (Beamforming) en frecuencias bajas, mejor sensibilidad de receptor a causa de MRC en frecuencias altas, múltiples flujos de transmisión y algunas otras ventajas de 802.11n, como combinación de canal y así sucesivamente. Los *access point* 1552 pueden proporcionar comparativamente celdas mas largas y capacidad superior.

IV.7.5.2.3. Consideraciones especiales para Redes Mesh de Interior

Tenga en cuenta estas consideraciones para las redes *Mesh* de interior:

- Voz sólo es sopotando con redes *Mesh* de interior. Para exterior, voz es soportado en base a mejor esfuerzo en la infraestructura *Mesh*.
- Calidad de Servicio (QoS) es soportado en el radio local de clientes 2,4 GHz y en 5 GHz y 4,9 GHz backhaul.
- Cisco también soporta static Call Admission Control (CAC) en clientes CCXv4, lo que proporciona CAC entre el *access point* y el cliente.
- Radio entre RAP y MAP. El radio recomendado es 3 a 4 MAPs por RAP.
- Distancia entre APs:
  - ✓ Para AP comunes 11n (1130 y 1240), una distancia de no más de 200 pies (60,96 metros) entre cada access point *Mesh* es recomendado, con un radio de celda de 100 pies (30,48 metros).
  - ✓ Para AP *Mesh* 11n (1040, 1140, 1250, 1260, 3500e y 3500i), una distancia de no más de 250 metros entre cada access point *Mesh* con un radio de celda de 125 metros es recomendado.
- Para conteo de saltos para datos, el máximo es de 4 saltos. Para voz se recomienda no más de dos saltos.
- Consideraciones de RF para el acceso de clientes en redes de voz:
  - ✓ Hoyos de cobertura de 2 a 10 %
  - ✓ Cobertura superpuesta de celdas de 15 a 20 %
  - ✓ Voz necesita valores RSSI y SNR que son al menos 15 dB más alto que los requerimientos de datos
  - ✓ RSSI de -67 dBm para todos los tipos de datos debe ser la meta de 11b/g/n y 11a/n
  - ✓ SNR debe ser de 25 dB para la velocidad de datos utilizado por el cliente para conectarse al AP
  - ✓ Tasa de error de paquete (PER) debe estar configurado para un valor de 1 % o menos
  - ✓ El canal con la menor utilización (CU) debe ser utilizado. Compruebe la CU cuando no haya tráfico que se este ejecutando.

- ✓ Administrador de recursos de radio (RRM) puede ser utilizado para implementar el recomendado RSSI, PER, SNR, CU, cobertura de celdas y configuración de hoyos de cobertura determinados para el radio 802.11b/g/n (RRM no está disponible en radios 802.11a/n).

IV.8. Equipos para la red WMN

Para la implementación del diseño de la Red Inalámbrica *Mesh*, se describen equipos basados en el estándar 802.11g/n, los mismos que permiten una estructura y una configuración Mesh y así permitir una mayor cobertura del sistema, cuando se desee brindar los servicios de Internet a usuarios externos al campus universitario. Se describen algunas opciones de equipos que puede tener el diseño de la red inalámbrica, se analizará las mejores alternativas que brinden una solución unificada y centralizada de los recursos, para permitir una fácil administración y escalabilidad de la red.

IV.8.1. Access Points Mesh

IV.8.1.1. Cisco Aironet 1552e (outdoor)

Figura IV.11 Acces Point Cisco Aironet 1552e

Access Point Inalámbrico de alto rendimiento al aire libre

El *Access Point* para exteriores de Cisco, Aironet serie 1550 con tecnología CleanAir. Es la primera empresa de la industria y con calidad de operador 802.11n, en crear auto-curación y auto-optimización de redes inalámbricas, que mitiga el impacto de las

interferencias inalámbricas. Ofrece una red *Mesh* flexible, segura y escalable de alto rendimiento, para movilidad en áreas metropolitanas de gran tamaño, recintos empresariales, zonas de fabricación y pozos mineros. El Cisco Aironet serie 1550, soporta múltiples dispositivos y múltiples aplicaciones de red y distribuye en tiempo real, la movilidad sin fisuras, video-vigilancia, 3° generación (3G) y 4º generación (4G) de descarga de datos y acceso WiFi, público y privado. Diseñado para satisfacer las necesidades de los clientes en una amplia gama de industrias, el Cisco Aironet serie 1550 ofrece los siguientes beneficios:

- ***Opciones flexibles deimplementación****:* Acceso a redes *Mesh*, extensión de una red *Ethernety Ethernet*, fibra, inalámbricas o cables de retorno.
- ***Soporte técnico del proveedor de servicios****:* WiFi móvil para descarga de datos de la siguiente generación y servicios móviles personalizados.
- ***Tecnología Cisco CleanAir****:* Inteligencia integrada del espectro para detectar, clasificar y mitigar la interferencia de RF no autorizado, de puentes inalámbricos o dispositivos maliciosos.
- Alto ancho de banda de video-vigilancia a través de WiFi, sin el alto costo de la instalación de cables a largas distancias.
- Alto rendimiento, red de usos múltiples con bajos gastos de capital y bajos gastos operativos.
- ***Integrado de cable e inalámbrico****:* La Arquitectura Cisco de redes sin frontera, proporciona ahorro en los costos, con soluciones de extremo a extremo que incluyen acceso a la red inalámbrica, con mutación, en rutamiento y seguridad.

Flexible, de alto rendimiento Mesh

El Access Point para exteriores Cisco Aironet serie 1550, ofrece una plataforma Mesh flexible, segura y escalable, que es parte de la red inalámbrica unificada de Cisco y del Servicio del proveedor de soluciones WiFi de Cisco. Ofrece alto rendimiento de movilidad en áreas metropolitanas de gran tamaño y recintos empresariales, zonas de fabricación y pozos mineros. El Cisco Aironet serie 1550, proporciona acceso de

dispositivos de alto rendimiento, a través de la sensibilidad de radio mejorada y el rango con tecnología 802.11a/b/g/n multiple-input multiple-output (MIMO), con dos flujos espaciales.

Están disponibles multiples enlaces ascendentes y opciones de energía. El 802.3af *Power-over-Ethernet* (PoE,) hace que sea fácil la conexión de dispositivos IP, como cámaras de vídeo IP. La caja NEMA4X, ayuda a garantizar un sistema robusto, que puede soportar los entornos más exigentes. Para ayudar a asegurar el tiempo de actividad para aplicaciones de misión crítica, incluso en el caso de que la energía eléctrica no esté disponible, el Cisco Aironet serie 1550, ofrece una batería interna de energía de reserva.

Tecnología Cisco CleanAir

El *Access Point* Cisco Aironet serie 1550, con tecnología Cisco CleanAir, proporciona la conectividad 802.11n de más alto rendimiento, para redes de misión crítica en ambientes libres, mediante la detección de interferencia de dispositivos no autorizados, así como las más comunes fuentes de interferencias en exteriores, tales como las redes WiMAX y productos inalámbricos de transición. La serie 1550, utiliza un chip de inteligencia para crear un espectro-consciente, auto-curación y auto-optimización de redes inalámbricas, que mitigan el impacto de la interferencia inalámbrica. CleanAir es una característica de todo el sistema de la red inalámbrica unificada de Cisco, que mejora la calidad de la red inalámbrica, mediante la detección de interferencias de RF que otros sistemas no pueden reconocer, identificando el origen, localización y luego realizando los ajustes automáticos para optimizar la cobertura inalámbrica.

Excelente RF

Basándose en la herencia de Cisco Aironet de excelente RF, el Cisco Aironet serie 1550, ofrece el mejor rendimiento de conexiones inalámbricas seguras y fiables. Partes: de clase industrial, de clase empresarial y de inteligencia a nivel de silicio y radios optimizados, ofrecen una experiencia de movilidad robusta. El Cisco Aironet serie 1550, ofrece un conjunto de herramientas que proporcionan una base sólida y la base

inalámbrica escalable requerida, para aprovechar el verdadero potencial de la movilidad inalámbrica al aire libre:

- Tecnología Cisco ClientLink, para elevar el rendimiento del enlace ascendente y descendente, de la cobertura de clientes existentes 802.11a/g
- Administración de los recursos de radio (Radio Resource Management), para seleccionar los canales automatizados y la gestión de configuración de energía de los *access points.*
- Capacidades avanzadas para seleccionar: flujos de datos, ajustes de potencia y gestionar la calidad de servicio (QoS) para *access points.*

Gestión Centralizada para redes Mesh

Gestión centralizada y resolución de problemas de los *Access Point* inalámbricos Cisco para exteriores, evitan las costosas llamadas de servicio de mantenimiento a los lugares al aire libre, El Cisco *Wireless Control System* (WCS) trabaja en conjunto con los *access points* Aironet de Cisco y las controladoras de LAN inalámbrica de Cisco, para configurar y administrar las redes inalámbricas. Con Cisco WCS, los administradores de red tienen una única solución para: la predicción de RF, la política de aprovisionamiento, la optimización de redes, resolución de problemas, control de seguridad y sistemas de gestión de LAN inalámbricas. La tecnología Cisco CleanAir, está integrada en el WCS para proporcionar información en tiempo real de su red exterior. La seguridad de la red inalámbrica, es también parte de una solución unificada de cable e inalámbrico. *Cisco Wireless Network Security,* ofrece el más alto nivel de seguridad de red, lo que ayuda a asegurar que los datos se mantengan en forma confidencial y segura y que la red esté protegida del acceso no autorizado

Access Point Cisco Aironet 1552E con antena externa

El *Access Point* para exteriores Cisco Aironet 1552E, es el modelo estándar, con sistema de doble radio, con radios de doble banda que son compatibles con los estándares IEEE 802.11a/n (5 GHz) y los estándares 802.11b/g/n (2,4 GHz). El 1552E, tiene tres

conexiones de antena externa, para tres antenas de doble banda. Tiene opciones de *backaul* con Ethernet y fibra (SFP), junto con la opción de batería de respaldo. Este modelo también cuenta con un puerto de salida PoE y puede suministrar energía a una cámara de video vigilancia. Un modelo muy flexible, el Cisco Aironet 1552E, está bien equipado para despliegues municipales y de campus, aplicaciones de vídeo vigilancia, entornos mineros y descarga de datos.

IV.8.1.2. Cisco Aironet 3500p (indoor)

Figura IV.12 Acces Point Cisco Aironet 3500p

Los *access points* Cisco Aironet 3500p, son los nuevos miembros de la serie 3500 con tecnología Cisco CleanAir. Es el primer sistema de la industria, en crear auto-curación y auto-optimización de redes inalámbricas 802.11n.

Implementaciones de alta densidad

El espectro de radiofrecuencia es limitado, con usuarios móviles que demandan una cantidad creciente de capacidad de ancho de banda, para vídeo y otras aplicaciones de alto consumo. En ambientes tales como estadios y arenas, proporcionar acceso WiFi consistente y confiable, puede ser un reto, especialmente, cuantos más dispositivos móviles están concentrados en un área confinada y con techos, altos o inexistentes, para la instalación de puntos de acceso.

El modelo 3500p, está diseñado con parámetros de configuración a medida y ancho de banda estrecho, con antenas externas de alta ganancia, para proporcionar cobertura seleccionada para implementaciones de alta densidad. Este sistema especial de antenas

direccionales y ajustes de potencia, facilitan a una organización desplegar más *access points* cercanos, permitiendo mayor capacidad, menor interferencia co-canal y una mejor experiencia de usuario. Debido a la única configuración de la antena y el poder, las regulaciones FCC requieren que el *Access Point* Cisco Aironet 3500p, sea instalado por un profesional certificado.

Excelente RF

Basándosé en la herencia Cisco Aironet de excelente RF, el modelo 3500p, ofrece un rendimiento líder en la industria, para las conexiones inalámbricas seguras y fiables. *Chipsets* de clase empresarial y radios optimizados, ofrecen una robusta experiencia en movilidad usando la tecnología Cisco M-Drive, que incluye:

- La tecnología **Cisco CleanAir** para detectar de forma inteligente y mitigar las interferencias de RF para un alto rendimiento 802.11n.
- La tecnología **Cisco ClientLink** para mejorar la fiabilidad y la cobertura para clientes.
- La tecnología **Cisco BandSelect** para mejorar las conexiones clientes de 5 GHz, en entornos de clientes mixtos.
- La tecnología **Cisco VideoStream**, que utiliza *multicast* para mejorar aplicaciones multimedia.

Escalabilidad

El *access point* Cisco Aironet 3500p, es un componente de la red inalámbrica unificada de Cisco, que puede escalar hasta 18.000 *access points*, con total movilidad de capa 3 en zonas céntricas o remotas en el: campus empresarial, en oficinas sucursales y en sitios remotos. La red inalambrica unificada de Cisco es la industria más flexible, resistente y escalable de una arquitectura de red inalámbrica, proporcionando acceso seguro, a los servicios de movilidad y de aplicaciones y ofrece el menor costo total de adquisición e inversión protegida, mediante la integración con la existente red cableada.

IV.8.2. Cisco Wireless LAN Controller 5500

Figura IV.13 Cisco Wireless LAN Controller 5500

El Cisco Wireless Controller serie 5500, es una plataforma altamente escalable y flexible, que permite un sistema amplio de servicios para ambientes inalámbricos, en medianas o grandes empresas y campus universitarios. Diseñado para un rendimiento 802.11n y escalabilidad máxima, la serie 5500, ofrece tiempo mejorado de actividad con visibilidad y protección de RF, la capacidad de manejar simultáneamente hasta 500 *access points*, un rendimiento superior para fiabilidad de *streaming* de vídeo y calidad de voz y la recuperación de errores, mejorada para una experiencia de movilidad constante en los entornos más exigentes.

Características

Optimizado para redes inalámbricas de alto rendimiento, la serie 5500, ofrece una mejor movilidad y prepara la empresa para la próxima ola de dispositivos y aplicaciones móviles. La serie 5500 soporta una mayor densidad de clientes y entrega un *roaming* más eficiente, con un mínimo de nueve veces el rendimiento de las redes existentes 802.11a/g. La serie 5500 automatiza la configuración inalámbrica y funciones de administración y permite a los administradores de red, tener la visibilidad y el control necesarios, para manejar de manera rentable, asegurando y optimizando el rendimiento de sus redes inalámbricas.

Con la tecnología integrada CleanAir, la serie 5500 protege el rendimiento de 802.11n, al ofrecer acceso a la red cruzada en tiempo real e información histórica de interferencia

de RF, para la rápida solución y resolución de problemas. Como un componente de la red inalámbrica unificada de Cisco, esta controladora ofrece, comunicación en tiempo real entre *access points* Cisco Aironet. El Cisco *Wireless Control System (*WCS) y el Cisco *Mobility Services Engine*, entregan políticas de seguridad centralizadas, sistema inalámbrico de prevención de intrusiones (IPS), mejora en la administración de RF y calidad de servicio (QoS).

IV.8.3. Cisco Wireless Control System (WCS)

Cisco *Wireless Control System* (WCS), es la plataforma de administración mas completa, en la industria de administración de ciclo de vida de 802.11n y 802.11a/b/g, de las redes inalámbricas de clase empresarial. Esta plataforma de administración robusta, ofrece una solución de administración costo-efectiva, que permite a los administradores de TI planificar, implementar, monitorear, solucionar problemas e informar sobre las redes inalámbricas en interiores y exteriores (Figura IV.13). Cómo la plataforma de administracion de Cisco *Unified Wireless Network*, Cisco WCS apoya la entrega de aplicaciones de alto rendimiento y soluciones de misión crítica, que simplifican las operaciones del negocio y mejoran la productividad.

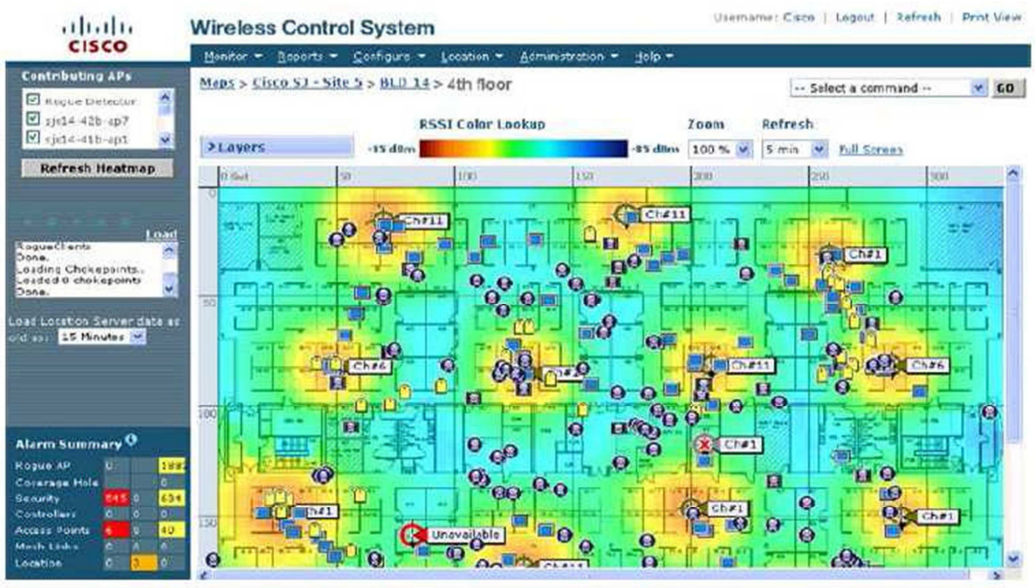

Figura IV.14 Wireless Control System (WCS)

También es compatible con la tecnología Cisco CleanAir, la capacidad de todo el sistema de Cisco *Unified Wireless Network*, que utiliza silicio a nivel de inteligencia, para crear una red inalámbrica con auto-curación y auto-optimización. Entrega protección de rendimiento para redes 802.11n. La tecnología Cisco CleanAir aumenta la fiabilidad de las redes inalámbricas, para apoyar las aplicaciones de misión-crítica mitigando automáticamente el impacto de interferencias de radiofrecuencia (RF). Cisco WCS es una plataforma completa, que se adapta para satisfacer las necesidades de las redes inalámbricas: pequeñas, medianas y grandes LANs, a través de redes locales y lugares remotos, nacionales e internacionales.

Esta premiada solución, ofrece a los administradores de TI, acceso inmediato a las herramientas que necesitan, cuando las necesitan y es la manera más eficiente de implementar y mantener segura LAN inalámbrica, todo desde una ubicación centralizada, que requiere un mínimo de personal de TI. Los costos operativos se han reducido significativamente a través de la intuitiva "interfaz gráfica de usuario" de Cisco WCS, por su simplicidad de uso y construido con herramientas que ofrecen una mejora de la eficiencia, bajos costos de capacitación y reducción de las necesidades de personal de TI, incluso si la red crece. A diferencia de la superposición de herramientas de administración, Cisco WCS reduce los costos operativos, mediante la incorporación de la amplitud de los requerimientos de administración, desde señales de radiofrecuencia, hasta los controladores de servicios, dentro de una única plataforma unificada.

Plataforma Flexible y fácil de usar

Cisco WCS es la plataforma ideal para la administración de nuevos y experimentados administradores de TI. Su facilidad de uso, sencillo e intuitivo, elimina la complejidad de la interfaz para usuarios, que requieren una experiencia de gestión automatizada, mientras completa funciones de administración de ciclo de vida, para satisfacer las necesidades, incluso, de los administradores mas avanzados de TI. Cisco WCS es inherentemente flexible, permitiendo que cada usuario pueda personalizar su interfaz de

administración, para mostrar sólo la información más relevante, que es requerida para cumplir con los objetivos operativos y del negocio.

Escalabilidad sin fisuras

Cisco WCS, escala para manejar cientos de controladoras LAN inalámbricas Cisco, que a su vez pueden gestionar miles de *access points* Cisco Aironet, incluyendo la próxima generación de *access points* 802.11n, Cisco Aironet 3500, 1260, 1250 y 1140 series. Para implementaciones a gran escala, en interiores y exteriores, Cisco WCS Navigator, se puede incluir al mismo tiempo, para soportar un máximo de 20 plataformas de Cisco WCS y 30.000 *access points* Cisco. Adicionando servicios de movilidad Cisco, tales como software sensible al contexto y sistema adaptativo de prevención de intrusión inalámbrica (WIPS), ésta se simplifica a través de la integración de, Cisco WCS con Cisco Mobility Services Engine (MSE).

IV.8.4. Cisco Catalyst 3750-X y 3560-X switches

Figura IV.15 Cisco Catalyst 3750-X y 3560-X switches

Los switches Cisco Catalyst serie 3750-X y 3560-X, son una línea de switches apilables e independientes de clase empresarial, respectivamente. Estos switches proporcionan alta disponibilidad, escalabilidad, seguridad, eficiencia energética y facilidad de uso, con características innovadoras, tales como: Cisco StackPower (disponible sólo en el catalyst 3750-X), configuraciones IEEE 802.3af Power over Ethernet Plus (PoE +), módulos de

red opcionales, fuentes de alimentación redundantes y características de seguridad Media Access Control (MACsec).

El Cisco Catalyst serie 3750-X, con tecnología *StackWise Plus*, proporciona escalabilidad, facilidad de administracion y protección de inversión para las necesidades cambiantes de la empresa. El Cisco Catalyst 3750-X y 3560-X, mejora la productividad mediante aplicaciones como: telefonía IP, comunicaciones inalámbricas y video, para una experiencia de red sin fronteras. Cisco Catalyst serie 3750-X y 3560-X, tiene las siguientes características principales:

- 24 y 48 puertos 10/100/1000 PoE + y modelos no PoE y 12 y 24 modelos de puerto GE SFP.
- Cuatro módulos de red opcionales *uplink* con puertos GE ó 10GE.
- Primero en la industria PoE + con 30W de potencia, en todos los puertos en un *rack* (RU) de factor de forma.
- Doble fuente modular de alimentación redundante y ventiladores.
- Media Access Control Security (MACsec), cifrado basado en hardware.
- NetFlow flexible y cifrado hardware de switch a switch, con el módulo de servicio *uplink.*
- Open Shortest Path First (OSPF) para el acceso enrutado en una imagen IP Base.
- Enrutamiento IPv4 e IPv6, enrutamiento multicast, calidad de servicio avanzada (QoS) y funciones de seguridad en hardware.
- Mejora de garantía limitada de por vida (LLW), con el siguiente día de trabajo (NBD) sustitución avanzada de hardware y 90 días de acceso al soporte Cisco Technical Assistance Center (TAC).
- Mejora de Cisco EnergyWise, para la optimización de los costos operativos, mediante la medición de consumo de energía real de los dispositivos PoE, informando y reduciendo el consumo de energía a través de la red.

- Puertos USB de tipo A y tipo B, para el almacenamiento y la consola, respectivamente y un puerto de administracion Ethernet fuera de banda.

Además de las características anteriores, el Cisco Catalyst 3750-X switches, también ofrece:

- **Tecnología Cisco StackPower**: Una característica innovadora y es la primera industria en compartir cantidad de poder entre la pila de miembros.
- **Tecnología Cisco StackWise Plus:** Para la facilidad de uso y capacidad de recuperación con 64 Gbps de rendimiento.
- Protección de la inversión, con la compatibilidad hacia atrás, con todos los demás modelos de la serie Cisco Catalyst serie 3750 swtiches.

IV.8.5. Cisco 3900 ISR Router

Figura IV.16 Cisco 3900 ISR Router

Los *routers* Cisco serie 3900 Integrated Services Routers (ISR), se basan en 25 años de innovación y liderazgo de productos de Cisco. La nueva plataforma Cisco *Integrated Services Routers Generation 2* (ISR G2), ha sido diseñada para permitir a la siguiente fase de evolución de *branch-office*, el proporcionar medios dinámicos colaboración y virtualización de la sucursal, al tiempo que maximiza el ahorro de costes operativos.

Los nuevos *routers* soportan, los nuevos procesadores de alta capacidad de señales digitales (DSP), para las futuras capacidades mejoradas de video, módulos de servicios de alto poder, con una mayor disponibilidad, CPUs multi-núcleo, Gigabit Ethernet switching con Cisco Enhanced Power over Ethernet (ePoE) y la nueva visibilidad de energía y capacidades de control, al tiempo que mejora el rendimiento general del sistema.

Además, una nueva imagen IOS de Cisco y Motor de Servicios Preparado (SRE), módulo que permite desacoplar el despliegue de hardware y software, proporcionando una base tecnológica flexible, que puede adaptarse rápidamentea la evolución de requisitos de la red. En general, la serie Cisco 3900, ofrece un coste total excepcional de ahorro de propiedad (TCO) y agilidad de la red a través de: la integración inteligente, líder en el mercado en seguridad, comunicaciones unificadas, soluciones inalámbricas y servicios de aplicación.

Descripción del producto

La serie Cisco 3900, se basa en la mejor oferta en su clase, de las ya existentes Cisco 3800 series, de Servicios integrados de *routers*. Ahora ofrece cuatro plataformas: el Cisco 3945E, Cisco 3925E, Cisco 3945 y Cisco 3925 ISR. La serie Cisco 3900, ofrece una aceleración de encriptación de hardware integrado, de voz y de vídeo con capacidad de ranuras de DSP, *firewall* opcional, prevención de intrusiones, procesamiento de llamadas, correo de voz y servicios de aplicación.

Además, las plataformas de soporte más amplias de la industria de cableado y opciones de conectividad inalámbrica, tales como: T1/E1, T3/E3, xDSL, cobre y fibra Gigabit Ethernet. La serie Cisco 3900 ofrece un rendimiento superior y flexibilidad para el despliegue de redes flexibles, de pequeñas oficinas de negocios hasta de las oficinas de grandes empresas. Todo ello proporciona la industria líder en protección de la inversión.

IV.9. Diagrama de la red WMN

El diagrama para incorporar la red WMN de la UPDS, está representado por las diferentes capacidades a brindar a cada usuario final, por tal motivo se describe el esquema estructurado de la red *Mesh,* para la red universitaria, el mismo que deberá satisfacer los requerimientos de todos los usuarios de la red.

Se implementará independientemente el diseño de la red *Mesh,* con la red LAN de la UPDS, ya que se emplearán algunos recursos que posee la red LAN actual de la Universidad, los mismos que permiten brindar ciertos servicios a la nueva red *Mesh* y poseen las características necesarias para trabajar en conjunto con la red propuesta.

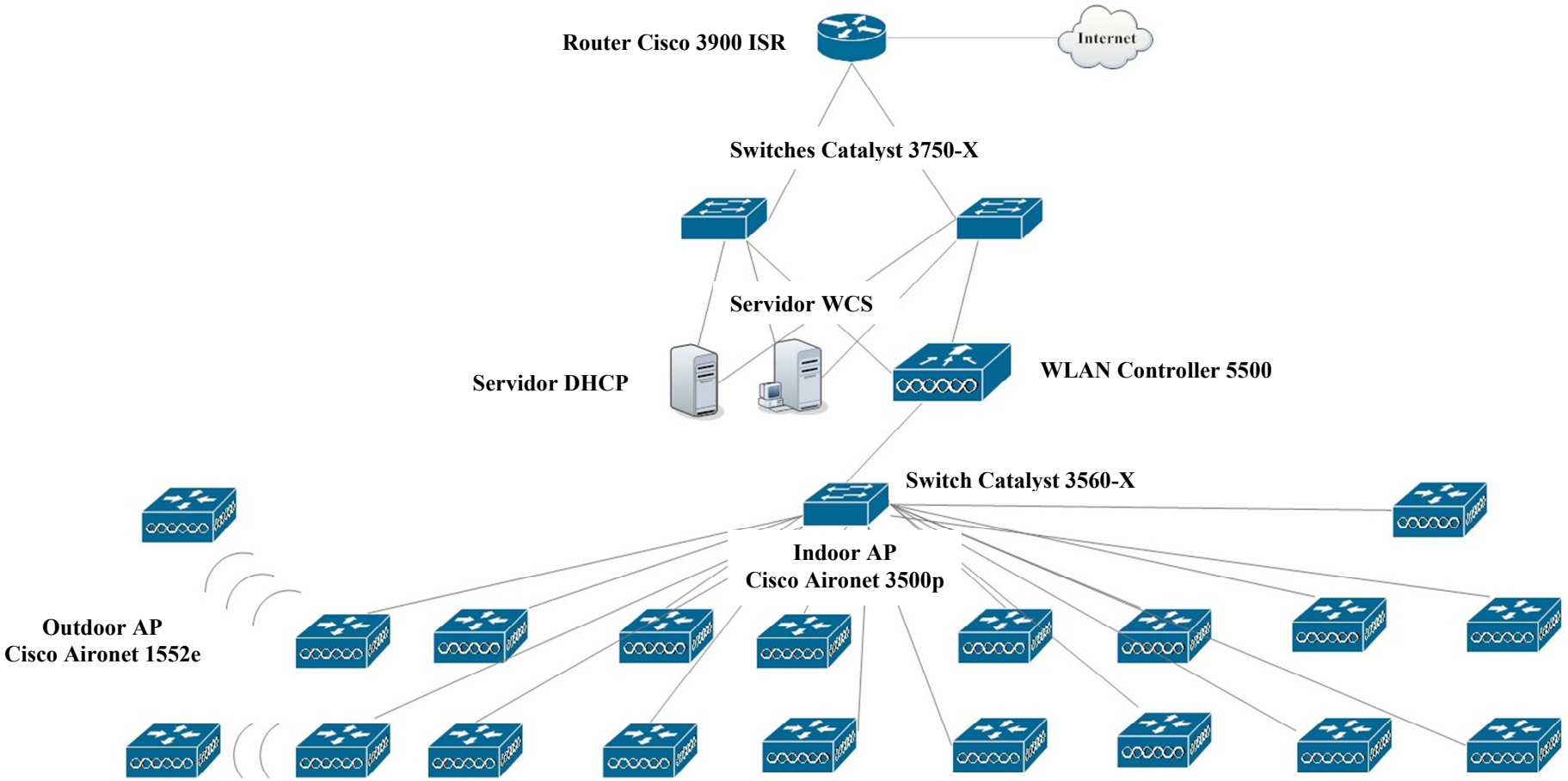

Figura IV.17 Diagrama de la red WMN

IV.10. Características Generales de la Red WMN

La arquitectura de la red inalámbrica *Mesh* para la Universidad Privada Domingo Savio, debe poseer ciertas características, de tal forma que la vuelvan una red eficiente y acorde a los requerimientos de cada usuario y que camine conjuntamente con el avance tecnológico.

IV.10.1. Roaming

El *roaming* se define, como la libertad para movilizarse libremente, dentro de un espacio determinado, sin que exista lapsos de interrupción entre la comunicación de los usuarios, cuando pasan de la cobertura de un punto de acceso, a la cobertura de otro. Para permitir la itinerancia (*roaming*) y movilidad de los usuarios, es necesario colocar los *Access Points,* de tal manera que haya "*overlapping*" o superposición entre los radios de cobertura.

Existen dos clases de *roaming*, cuando un usuario cambia de un punto de acceso a otro, reasociándose con este nuevo punto de acceso, pero que pertenece a la misma subred. El cambio entre diferentes puntos de acceso, que se encuentran en otros niveles de red (subredes), se denomina *roaming* de capa 3.

IV.10.2. Balanceo de Carga

El protocolo LWAPP, permite el balanceo de carga dinámico, entre los puntos de acceso asociados a una controladora para aumentar el rendimiento. Las controladoras tienen acceso a la potencia de señal que hay en los puntos de acceso. Cuando un cliente quiere asociarse a un punto de acceso, la controladora tiene acceso a la cantidad de señal, que recibe el cliente de los diferentes APs, entonces, la controladora escoge qué punto de acceso, es el más adecuado para el cliente, en función de la potencia y la relación señal-ruido (SNR).

IV.10.3. Autenticación de Usuarios

Antes de tener acceso a los recursos de la red, los usuarios deben ser autenticados.

El acceso a cada uno de los usuarios, debe proveer administración de claves, tanto del lado del sistema de acceso como del cliente, para asegurar que se conectará a la red propia y evitar posibles amenazas o problemas.

IV.10.4. Redundancia

La redundancia en el diseño, permitirá brindar confiabilidad y seguridad, al momento de ofrecer los servicios de red e Internet a sus usuarios. Es un factor clave para el desarrollo y desenvolvimiento de la red, donde este tipo de sistemas, se encargan de realizar el mismo proceso en más de una estación, ya que si por algún motivo, alguno dejara de funcionar o se colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior. En el momento en que un dispositivo falla, la red continúa funcionando, de acuerdo al nivel de respaldo que se tenga y todo este proceso proporciona redundancia, eliminando ese punto de fallo. Otro punto importante en el diseño, es poder tener una redundancia lógica y física, con cada uno de los equipos o elementos más importantes, que además gestionan y administran a la red.

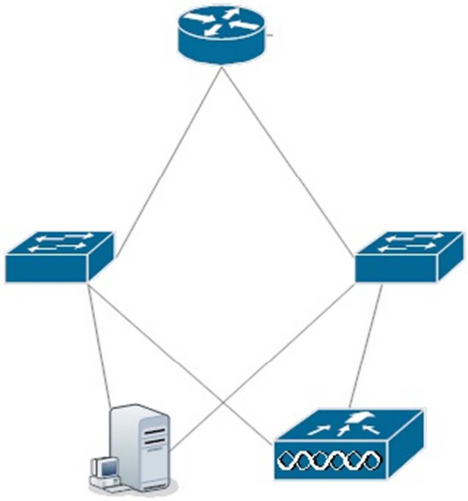

Figura IV.18 Redundancia de la red WMN

Además la red inalámbrica *Mesh* se caracterizará por ser tolerante a fallos, ya que si existiera algún problema en un nodo, tomarían los paquetes de datos automáticamente

caminos alternativos, garantizando el acceso de los usuarios a la red. Además en la Solución Unificada de Cisco, cuando cada *access point* detecta una falla en algún otro *access point*, se recurre a la detección de zonas sin cobertura, incrementando la potencia de los APs aledaños, para cubrir dichas zonas.

IV.10.5. Escalabilidad de la Red

El bajo costo de instalación, es una de las grandes ventajas de las redes de acceso inalámbricas. La escalabilidad de ellas se determina por factores como:

- El incremento de la zona de cobertura.
- El incremento del ancho de banda necesario y del número de usuarios, de acuerdo al ancho de banda designado.

En el primer caso, la única alternativa posible, consiste en instalar nuevos *Access Points*, considerando que el aumento de potencia en algunos de ellos, no pudiera dar servicio a la nueva zona por cubrir. En el segundo caso pueden plantearse más alternativas:

- Aumentar el número de portadoras utilizadas en un determinado sector. Duplicando el número de portadoras dentro de un sector, se duplica la anchura de banda disponible para los usuarios de dicho sector. La limitación en este caso, vendría impuesta por el número de portadoras disponibles en esa ubicación.
- Aumentar el número de sectores de un *Access Point*. En caso de no disponer de portadoras adicionales, podría optarse por desdoblar un sector en varios, aumentando con ello la capacidad efectiva del *Access Point.*

El problema a resolver en este caso, sigue siendo la limitación en el espectro disponible, puesto que habría que replantearse, para dicho *Access Point*, el esquema de reutilización de frecuencia utilizado, de forma que no se produzcan interferencias en los sectores ya existentes. En donde ninguno de los métodos anteriores fuera viable, podría optarse por aumentar el número de *Access Point*, de forma que el número de usuarios asignado a

cada una de ellas, se redujese, aumentando por tanto el caudal efectivo por usuario. Para conseguirlo, es necesario reducir la potencia de transmisión del *Access Point*, con lo cual se disminuye la zona de cobertura de la misma.

De esta manera, la Plataforma Unificada propuesta en el diseño, permitirá obtener una escalabilidad de la red y conforme aumente el número de usuarios y la cobertura de la red, se tendrá que aumentar el número de *Access Point* y sistemas de control, en donde el crecimiento de la red inalámbrica *Mesh* resulte más factible y fácil de realizarlo. No se tendrá que volver a reestructurar el modelo de la red en su totalidad, ya que el esquema por jerarquías de la red, permitirá implementar más elementos que se necesitaren en cada nivel, para así poder ampliar la cobertura de servicios hacia más usuarios, permitiendo un funcionamiento seguro y muy confiable, sin la necesidad de configurar nuevamente el diseño original. Además la arquitectura tipo *Mesh*, también brinda la posibilidad de aumento y escalabilidad de cualquier red inalámbrica, donde cada *Access Point* es, además independiente, en la medida en que puede decidir, la ruta que seguirá cada paquete de información en cada momento y más aun, cuando se produce un corte, el propio nodo es capaz de decidir cómo volver a trazar la ruta.

IV.11. Políticas de Seguridad definidas para la red WMN

Para procurar un desempeño óptimo en el desenvolvimiento del sistema y evitar cualquier problema de la red, se describen políticas de seguridad, que permitirán mantener un nivel de protección de cada uno de los recursos y evitar un uso indebido de la información que posee la red. Seguidamente se describen algunas políticas de seguridad:

- Cada equipo activo, que se encuentra ubicado dentro de los bloques, poseerá un lugar único y adecuado para su implementación con las respectivas seguridades.
- El acceso a los equipos de la red inalambrica *Mesh*, será controlado mediante alarmas y dispositivos de vigilancia y únicamente podrán tener acceso el personal autorizado.

- El diseño de la red inalámbrica para el acceso a Internet, incluye la autenticación de los usuarios mediante contraseñas, empleando el uso de claves compartidas y filtrado de direcciones MAC.
- Los usuarios inalámbricos del sector estudiantil, podrán acceder al Internet mediante el registro de sus direcciones MAC y tras un tiempo determinado de inactividad, sus registros serán eliminados y tomados como usuarios que ya no pertenecen a la universidad. En cambio los usuarios con cuentas y el sector docente, tendrán acceso a Internet mediante claves de autenticación.
- Se limitará el acceso y descarga de archivos en cualquier formato, para los usuarios del sector estudiantil y para el sector docente, se permitirá éste servicio, por ser otro tipo de clientes.
- El acceso a Internet, conlleva a la infección de un sinnúmero de virus, por parte de los terminales de los usuarios, por lo que se implementará un solo "antivirus" para la comunidad, el cuál debe poseer características superiores y mejores.
- Cada *Access Point* será debidamente ubicado, donde no pueda ser fácilmente manipulado por personas ajenas y se realizará una inspección de cada uno de ellos constantemente.
- Se concienciará a los usuarios de la red, al uso debido de los recursos, mediante políticas de acceso prohibido a ciertas páginas restringidas.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES Y RECOMENDACIONES

V.1. Conclusiones

Luego de haber concluido el presente proyecto denominado: "AMPLIACIÓN DE LA COBERTURA DE CONEXIÓN A LA RED DEL CAMPUS DE LA UPDS, UTILIZANDO TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC), COMO RECURSO PEDAGÓGICO EN EL PROCESO DE ENSEÑANZA-APRENDIZAJE (PEA)." en la Universidad Privada Domingo Savio, con el fin de incorporar Tecnologias de Información y Comunicación (TIC) en la misma, se llegó a las siguientes conclusiones:

- Con el diseño de la red inalambrica *Mesh*, se garantiza conectividad constante y sin interrupciones a la red e Internet en todos los predios del campus universitario de la UPDS, con una velocidad de transferencia de datos de 54 Mbps, cumpliendo con el estándar 802.11g, que satisface las necesidades de los usuarios.
- Debido a la inexistencia de un estándar final para implementaciones de redes inalámbricas *Mesh,* se tomaron los requisitos necesarios, de acuerdo al fabricante de los dispositivos de red elegidos.
- La topología en malla usada en el diseño de la red inalámbrica, permitirá la escalabilidad de la red y debido a que es una universidad nueva que está en crecimiento, le permitirá tener una larga vida útil, antes de necesitar de una actualización.
- El diseño de la red, se hizo en base a la *Plataforma Unificada de Cisco*, por ser una de las marcas mas reconocidas mundialmente.
- El diseño de la red inalámbrica *Mesh,* permitirá movilidad y conectividad constante, desde cualquier punto dentro del campus universitario, brindando un servicio rápido y eficaz de conexión a la red e Internet.
- La redundancia constituye un respaldo, ante la posible falla de cualquier punto de la red y que ha de evitar la interrupción de los servicios y aplicaciones que se

encuentren en proceso. De esta manera, se implementará la redundancia de equipos en la red inalámbrica *Mesh* para la UPDS.

- Los nuevos *Access Points* Aironet 1552 y 3500 de *Cisco,* permitirán a la red inalámbrica, obtener una configuración tipo *Mesh*, ya que poseen dos radios para poder tener este esquema. El primer radio del *access point,* brinda el acceso de los usuarios a la red, mientras que el segundo radio, realizará los enlaces de malla hacia otros *access points* de iguales características.
- La calidad de servicio, es una característica que presenta, cada uno de los equipos seleccionados para el diseño de la red inalámbrica *Mesh*, la misma que se implementará gracias al estándar 802.11e de las redes WLAN.
- El impacto de las TIC ofrece: verificación de oportunidades, mejora de tecnología, aumento de productividad y además -hoy en día su utilidad en la educación universitaria ha cambiado la forma de enseñanza-aprendizaje - la metodología que se conoce como "*e-learning"*.

Por otro lado, el desarrollo del proyecto ha concluido con la obtención de un diseño, que cumple con el propósito y objetivo trazado al inicio del proceso de desarrollo, descrito en el Capitulo I, permitiendo de esta forma, coadyuvar en la solución del problema de conectividad de la universidad, brindando una propuesta de implementación de red con tecnología actual.

V.2. Recomendaciones

A continuación se presentan algunas recomendaciones a tomar en cuenta, para el diseño de la red:

- Se debe implementar Políticas de Seguridad, debido a que la tecnología *Mesh,* permite que un equipo inalámbrico pueda tener acceso a la red sin mayor problema. También se hacen necesarias: políticas de configuración de equipos, políticas de acceso remoto, políticas de contraseñas, etc., que son necesarias para reducir el ingreso a la red, de usuarios no deseados.

- Se recomienda hacer un “análisis de tráfico” para este tipo de redes, ya que dicho análisis escapa al alcance de esta tesis, pero que sin embargo es importante realizarlo, pues este análisis permitirá tener una idea más clara del comportamiento de la red y poder así realizar modificaciones en el diseño, antes de que la red se implemente físicamente.
- Llegar a establecer políticas de seguridad dentro de la red para los usuarios. Es una alternativa que debe tener muy en cuenta la Universidad Privada Domingo Savio, de manera que se informe a cada usuario, de los riesgos que implicarían para el bienestar de la Universidad, violar estos acuerdos.
- El número de usuarios de la red, debe ser equitativa a la calidad y capacidad que preste la misma, siendo el factor principal, cubrir las necesidades de los usuarios con calidad de servicio.