ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

"Estudio y diseño de un nodo de acceso, que sirva como piloto para la implementación de una red Wireless Mesh en la Facultad de Ingeniería en Electricidad y Computación de la ESPOL"

INFORME DE PROYECTO DE GRADUACIÓN

Previa la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Milton Ivan Cañarte Manrique

Daniel Alexander Parra Loayza

GUAYAQUIL – ECUADOR

AÑO 2009

AGRADECIMIENTO

A Dios por bendecirnos para llegar al lugar donde hemos llegado.

A nuestras familias que han estado con nosotros todo el tiempo brindando su apoyo y cariño.

A nuestro director de tesis, Ing. Ronald Ponguillo por su valiosa asesoría.

A un gran amigo, Ing. Vicente Paredes por todos los conocimientos que compartió y por su valioso tiempo que dedicó a nuestras inquietudes.

A todos aquellos que creyeron en nosotros.

DEDICATORIA

A Dios por iluminarme el camino y ubicarme en el tiempo y en lugar exacto. A mi familia por ser fuente de inspiración, apoyo incondicional y muestra de valores. A todas las personas que de una u otra manera me ayudaron en la vida universitaria

Milton Cañarte

A Dios por la vida y oportunidad que nos brinda día a día, a los seres más importantes en este mundo: mis padres, por ser la fuente de motivación para superarme cada día, y a todas aquellas personas que estuvieron ahí para no decaer, brindando todo su apoyo.

Daniel Parra

TRIBUNAL DE SUSTENTACIÓN

MSc. Jorge Aragundi R. Presidente del Tribunal	Ing. Ronald Ponguillo I. Director de Proyecto de Graduación
MSc. Rebeca Estrada P. Miembro Principal	MSc. Ivonne Martin M. Miembro Principal

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este trabajo, nos corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”.

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Milton Ivan Cañarte Manrique

Daniel Alexander Parra Loayza

RESUMEN

El proyecto “Estudio y diseño de un nodo de acceso, que sirva como piloto para la implementación de una red Wireless Mesh en la Facultad de Ingeniería en Electricidad y Computación de la ESPOL” para lograr los objetivos se dividirá en cinco capítulos.

En el capítulo 1 se describen de forma general a las redes inalámbricas, los escenarios de aplicación, clasificación y estándares de las mismas, con esto se nota que las redes inalámbricas se han convertido en importantes y necesarias para el desarrollo de una sociedad.

En el capítulo 2 se menciona las características, sistemas mallados, arquitectura, estándares, protocolos, capas del modelo OSI, calidad de servicio, seguridad, equidad y balanceo, consideraciones de las redes wireless mesh, con esto se logra comprender que son las WMN y cómo trabajan.

En el capítulo 3 se describe el área de la FIEC como el área de estudio, se realiza un análisis de los proveedores de soluciones mesh, se elige a Nortel como proveedor de los equipos mesh para realizar el diseño, se menciona las características, elementos, calidad de servicio y estrategias de diseño para las redes mesh de Nortel. Además se muestra la topología, el direccionamiento IP y el diagrama de la red mesh diseñada para la FIEC.

En el capítulo 4 se simula la solución planteada con ayuda del Planner, software de Nortel, se presenta los resultados de cobertura de la red y la solución en 3D. Además se plantea una nueva ubicación de los APs para mejorar la cobertura de la red y se comparan los resultados teóricos y prácticos de la solución mesh.

En el capítulo 5 se realiza un prototipo de un nodo de la solución, se muestra los equipos y las direcciones IPs utilizadas en la configuración de la red. Además se realizan las pruebas de conectividad entre los equipos utilizados en el nodo mesh y se compara resultados teóricos, prácticos y simulados.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

En la actualidad se ha visto un avance importante en las telecomunicaciones más aún en el acceso a las redes de manera inalámbrica [1], en la cual tenemos una de las tecnologías más recientes como lo es Wireless Mesh Networks (WMN), que está siendo implementada en diversas zonas rurales, urbanas y campus universitarios de Estados Unidos y Europa con resultados exitosos.

“Wireless Mesh Network es una variante del WiFi tradicional y una extensión de las redes Ad-Hoc, en la que las clásicas celdas WiFi basadas en cableado Ethernet hasta el switch se sustituyen por una red mallada” [2], donde los nodos se comunican entre sí sin cables, estableciendo una macro-burbuja de cobertura que puede cubrir desde un área pequeña hasta un área relativamente grande.

La red mallada de las WMN permite dar servicios a usuarios móviles, a semejanza de los sistemas celulares. Esta red mallada se crea haciendo la interconexión entre celdas de forma inalámbrica utilizando la banda de frecuencias de 5GHz, cada celda puede dar servicio utilizando la banda de frecuencias de 2,4GHz.

En la actualidad en Latino América y en todo el Ecuador se ha visto una alta demanda de servicios de telecomunicaciones [3], así como también la adquisición de equipos de última tecnología como celulares, laptops y agendas electrónicas que permiten acceso a internet de manera inalámbrica, esto muestra el interés y la necesidad que tienen las personas de comunicarse entre sí o simplemente navegar en internet.

También se ha notado que los usuarios de servicios de telecomunicaciones prefieren tener un acceso a la red de manera inalámbrica por diferentes razones:

- Evitar el robo de cable.
- Por estética.
- Por ser móvil.

Por las necesidades que hemos nombrado y el interés por mejorar las telecomunicaciones con sistemas inalámbricos hemos elegido como tema de tesis ***Estudio y diseño de un nodo de acceso, que sirva como piloto para***

la implementación de una red Wireless Mesh en la Facultad de Ingeniería en Electricidad y Computación de la ESPOL, en el cual mostraremos las ventajas de esta tecnología frente a otras tecnologías inalámbricas y sus características principales de ésta.

En el desarrollo del tema haremos un estudio del estado del arte de las redes wireless mesh, en el cual explicaremos lo que es una red Wireless Mesh así como también los puntos importantes de ésta, protocolos y los equipos necesarios para desarrollar la red mallada de un determinado proveedor (escogidos de un análisis).

Como un ejemplo de que la tecnología es robusta y eficiente, haremos un estudio y diseño de una red en la Facultad de Ingeniería Eléctrica y Computación, así lograremos tener un piloto que podría ser aplicado en un futuro en nuestra facultad.

Además haremos una simulación de la infraestructura diseñada para demostrar las ventajas y factibilidad de tener ésta tecnología en la ESPOL.

Al final desarrollaremos un prototipo, el cual nos permitirá comparar datos teóricos, simulados y reales.

CAPITULO 1

1. REDES INALÁMBRICAS O WIRELESS NETWORKS

1.1 INTRODUCCIÓN

Las redes inalámbricas permiten interconectar dos o más dispositivos usando como medio de comunicación ondas electromagnéticas. Las técnicas utilizadas en este tipo de redes son: infrarrojos, microondas, láser y radio, evitando el uso de redes cableadas.

En los últimos años, las redes inalámbricas han experimentado un importante auge debido a la introducción en el mercado de dispositivos basados en la serie de normas 802.11; que son baratos y fáciles de utilizar.

Estas redes permiten que el usuario, sin perder la conexión a internet o a alguna red privada, tenga flexibilidad y movilidad. Estas características han motivado a que existan investigaciones dedicadas a mejorar y desarrollar nuevas tecnologías inalámbricas.

1.2 ESCENARIOS DONDE LAS REDES INALÁMBRICAS SON UNA ALTERNATIVA INTERESANTE

Las redes inalámbricas son necesarias y toman ventaja frente a una infraestructura cableada cuando:

- En el lugar donde se desea implementar la red, el tendido de cable es costoso o prohibido.
- Se necesitan instalaciones temporales, por ejemplo en un cambio de oficina por un corto tiempo.
- Existe saturación de cables, ya sea por líneas telefónicas o la red eléctrica.
- Los usuarios son móviles y necesitan tener acceso a la red.
- La red se implementa en zonas donde el índice de robo de cable es muy alto.

1.3 CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las redes inalámbricas se las puede clasificar en tres categorías:

- WAN/MAN (Wide Area Network/Metropolitan Area Network).
- LAN (Local Area Network).

- PAN (Personal Area Network).

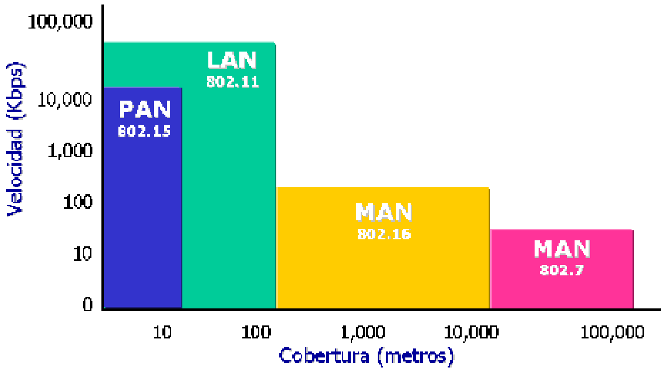


Figura 1-1 Velocidad Vs. Cobertura

En la figura anterior se muestra la comparación de la velocidad con respecto a la cobertura de cada categoría de las redes inalámbricas. Las redes WAN/MAN cubren desde decenas hasta miles de kilómetros, las redes LAN cubren desde metros hasta decenas de metros y la última categoría, las redes PAN cubren hasta 30 metros.

1.4 REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN)

Los esfuerzos por desarrollar una tecnología inalámbrica permitió crear estándares de área local ampliamente aceptados como Ethernet dieron sus frutos en lo que se conoce como WLAN o Redes de Área Local Inalámbricas, las cuales se basan en la familia de estándares IEEE 802.11.

Las principales topologías de redes WLAN son:

- Redes de Infraestructura.
- Redes Móviles Ad-hoc.
- Redes Inalámbricas de Tipo Malla.

1.4.1 REDES DE INFRAESTRUCTURA

Las redes de infraestructura se caracterizan por usar puntos de acceso (AP), que se encargan de proporcionar conexión entre nodos móviles dentro de la red inalámbrica o hacia el Internet.

En este tipo de topología, la tarjeta de red, laptop o cualquier dispositivo WiFi se configura automáticamente para usar el mismo canal radio que usa el punto de acceso más adecuado (normalmente el más cercano).

Este tipo de redes se utiliza generalmente cuando se necesita conectar una red WLAN a una red cableada.

Ventaja:

Reduce la complejidad de los nodos móviles dado que las estaciones no necesitan mantener información de los nodos vecinos.

Desventaja:

Requiere que todos los nodos estén dentro del área de cobertura del punto de acceso.

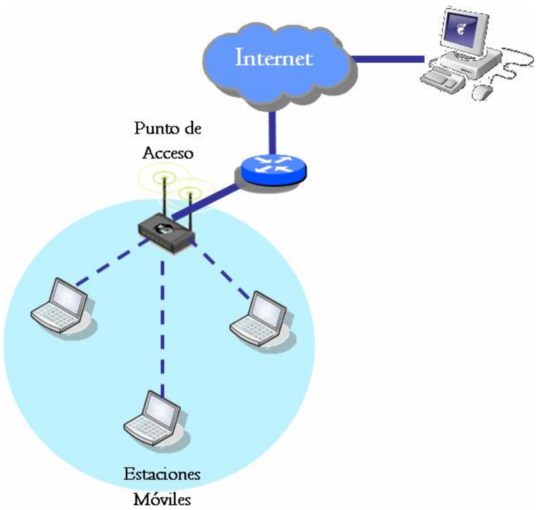


Figura 1-2 Red de Infraestructura

1.4.2 REDES MÓVILES AD-HOC

Las redes Ad-Hoc (mobile ad-hoc network o manet) se identifican porque al tener un conjunto de nodos móviles, éstos se comunican entre sí directamente sin necesidad de tener un punto de coordinación central o de acceso (AP), este tipo de redes pueden surgir de forma espontánea.

En este tipo de topología, las laptops o dispositivos WiFi de la red inalámbrica que quieren comunicarse entre ellos necesitan usar el mismo canal radio y configurar un identificar específico de WiFi llamado ESSID en Modo Ad-Hoc.

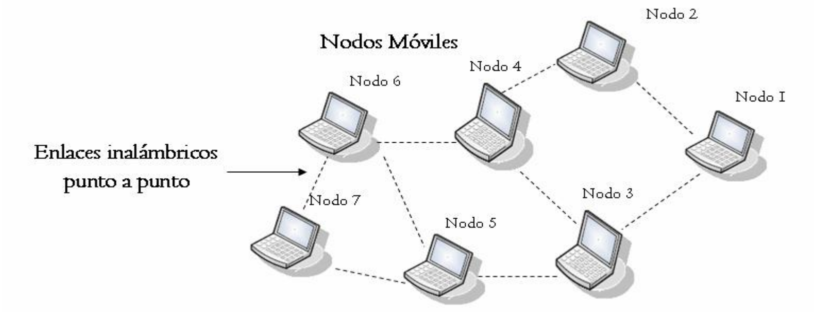


Figura 1-3 Red Inalámbrica ad-hoc

1.4.3 REDES INALÁMBRICAS DE TIPO MALLA

Las redes inalámbricas de tipo malla o Wireless Mesh Networks (WMN) son una extensión de las redes Ad-Hoc, se componen de nodos malla donde se encuentran los routers mesh, estaciones móviles o clientes mesh, y portales de acceso hacia la red cableada.

Las WMN se caracterizan por ser redes autoorganizadas dinámicamente, auto-regenerables y autoconfigurables, permitiendo tener grandes ventajas como robustez, confiabilidad y un fácil mantenimiento.

Entre los principales objetivos de las redes inalámbricas de tipo malla se encuentra el extender el área de cobertura, sin sacrificar la capacidad de canal, por esta razón los nodos malla están normalmente equipados con interfaces múltiples, las cuales pueden ser incluso de diferentes tecnologías de acceso inalámbrico.

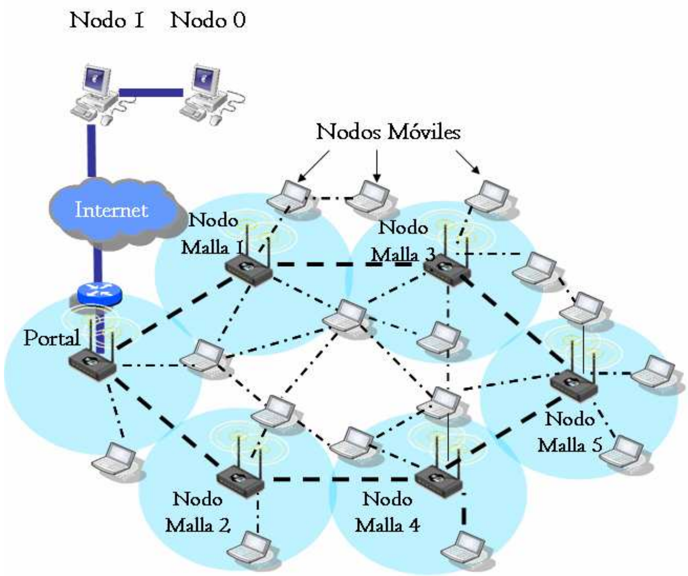


Figura 1-4 Arquitectura de Red Inalámbrica de Tipo Malla.

1.5 ESTANDARIZACIÓN DE LAS REDES INALÁMBRICAS DE ÁREA LOCAL WLAN

Tal como en el mundo de las redes cableadas, las redes WLAN cumplen con estándares genéricos para su funcionamiento, pero éstas necesitan normas adicionales específicas que definan el uso de los recursos radioeléctricos.

Dichas normas definen de forma detallada los protocolos de la capa física (PHY) y de la capa de enlace de datos que regulan la conexión vía radio. En la Figura 1-5 se muestra las capas mencionadas.

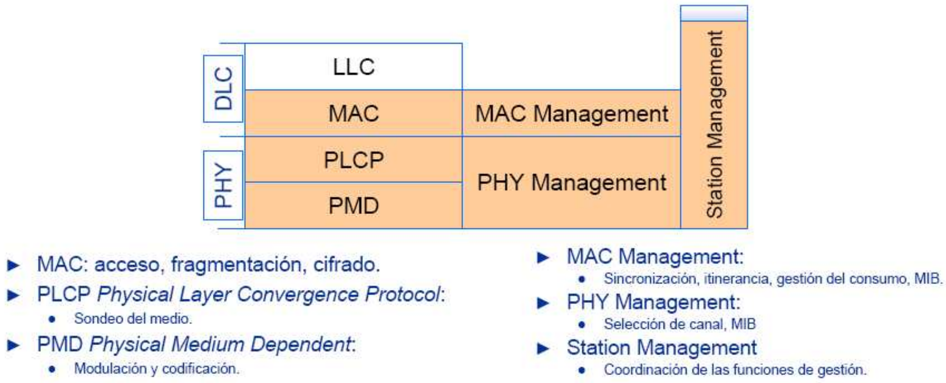


Figura 1-5 IEEE 802.11: Capas.

La capa física (PHY) de los estándares IEEE 802.11 se diseñó para cumplir con la regulación de radio frecuencia del FCC (organismo federal EEUU). Las mismas bandas de frecuencia, con algunas variantes, se utilizan en el resto del mundo.

En 1997 se generó el primer estándar de WLAN, fue desarrollado por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) y se lo denominó IEEE 802.11. Desde entonces varios organismos internacionales se han dedicado a desarrollar estándares para las WLAN. En Estados Unidos se encuentra al ya mencionado IEEE con el estándar 802.11 y sus variantes y en Europa el ETSI con sus actividades en Hiperlan-LAN.

En la Tabla I, se muestra los principales estándares de la especificación de redes WLAN IEEE 802.11 y algunas características de éstos.

Tabla I: Estándares de la especificación de redes WLAN IEEE 802.11

Estándar	Alcance del estándar
802.11a	Red WLAN de 54 Mbps,5Ghz
802.11b	11Mbps, 2.4Ghz
802.11e	Calidad de servicio (QoS)
802.11g	Red WLAN de 54Mbps, 2.4Ghz
802.11h	Administración del espectro (802.11a)
802.11n	Mejora Velocidad de Transmisión: Tecnología MIMO
802.11i	Seguridad y cifrado del estándar básico: Seguridad-AES
802.11k	Medición de recursos
802.11s	Redes en Malla

1.5.1 ESTÁNDAR IEEE 802.11

- Versión original del estándar IEEE 802.11, publicada en 1997.
- Alcanza un ancho de banda máximo de hasta 2 Mbps.
- Funciona en el espectro de 2,4 GHz sin necesidad de licencia (también referido como banda de ISM, Industry Science and Medical).
- Utiliza los sistemas de modulación FHSS (Frequency Hopped Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum).
- Define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso.

1.5.2 ESTÁNDAR IEEE 802.11a

- Ratificado en julio de 1999 (los productos comerciales comienzan a aparecer a mediados de 2002).
- Alcanza una velocidad máxima de 54 Mbps en la banda de 5 GHz.
- Utiliza modulación QAM-64 y codificación OFDM (Orthogonal Frequency Division Multiplexing).
- Como método de acceso aplica CSMA/CA.
- Trabaja con niveles de potencia emitida de 50 mW, 259 mW y 1 W.
- No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

1.5.3 ESTÁNDAR IEEE 802.11b

- Ratificado en 1999 y es el estándar principal de las redes inalámbricas.
- Tiene una velocidad máxima de transmisión de 11 Mbit/s.

- Como método de acceso utiliza CSMA/CA o RTS/CTS (Request to Send/Clear to Send), 4-Way Handshake.
- Opera dentro de la banda ISM 2.4 GHz.
- Utiliza modulación DSSS y modulación con forma de onda CCK (Complementary Code Keying).
- Trabaja con niveles de potencia emitida próximos a los 100 mW.

1.5.4 ESTÁNDAR IEEE 802.11g

- Publicada el 2002, es la tercera norma WLAN de IEEE 802.11.
- Permite transmitir a velocidades de hasta 54 Mbps.
- Utiliza modulación DSSS y codificación OFDM.
- Operada en la banda ISM 2.4 GHz.
- Los niveles de potencia emitida son próximos a los 100mW.
- Compatible con 802.11b e incompatible con 802.11a.

1.5.5 ESTÁNDAR IEEE 802.11e

- Dirige los requerimientos de calidad de servicio (QoS) para todas las interfaces de radio WLAN del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
- Diseñado para el soporte multimedia mejorado, garantizando la QoS en comunicaciones de gran ancho de banda y tiempo real (vídeo) en todo tipo de entornos y situaciones.
- Para ofrecer la calidad de servicio se introduce en el estándar IEEE 802.11e un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:
    - (EDCA) Enhanced Distributed Channel Access y
    - (HCCA) Controlled Access.

1.5.6 ESTÁNDAR IEEE 802.11i

- Está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación).

- Se basa en el AES (estándar de cifrado avanzado) como base para la seguridad, éste es un algoritmo de cifrado que soporta claves de 128, 192 y 256 bits, y puede cifrar transmisiones que se ejecutan en los estándares físicos a, b y g de 802.11.

- Por el empleo del AES los equipos requerirán mayor potencia en los procesadores de sus tarjetas y en los puntos de acceso.

1.5.7 ESTÁNDAR IEEE 802.11f

- El objetivo es lograr la interoperabilidad inalámbrica en puntos de acceso de distintos fabricantes desplegados.

- Es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP (Inter Access Point Protocol) 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.

1.5.8 ESTÁNDAR IEEE 802.11h

- Está disponible desde el año 2003.

- Desarrollado por exigencia de la Unión Europea para la autorización de operación del estándar 802.11a (manejo de la banda de 5GHz).

- Además el estándar 802.11h cumple con los reglamentos europeos para la banda de 5 GHz, que recomiendan que los productos tengan control de la potencia de transmisión (TPC) y puedan seleccionar frecuencia dinámicamente (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

1.5.9 ESTÁNDAR IEEE 802.11n

- La velocidad real de transmisión podría llegar a los 600 Mbps:

  * 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g.

  * 40 veces más rápida que una red bajo el estándar 802.11b.

- Utiliza tecnología MIMO (Multiple Input – Multiple Output), que ayudará a obtener un alcance de operación de las redes mayor que los anteriores estándares.

- Puede trabajar en dos bandas de frecuencias: 2,4 GHz y 5 GHz, lo que hace que este estándar sea compatible con dispositivos basados en los estándares anteriores.

1.5.10 ESTÁNDAR IEEE 802.11s

- Define la interoperabilidad de fabricantes en cuanto a protocolos Mesh. Se lo diseño para estandarizar las redes en malla ya que cada fabricante tiene sus propios mecanismos de generarlas.

- El estándar ofrece 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.

- Especifica en algunos esquemas de priorización de calidad de servicio (802.11e), medición de recursos de radio (802.11k) y administración del espectro (802.11h).

Además provee características de descubrimiento extendido de mallas con autoconfiguración automática y seguridad (802.11i).

1.6 REDES INALÁMBRICAS MULTIHOP

Este tipo de redes se caracterizan por usar una retransmisión inalámbrica de uno o varios saltos. Se las puede dividir en las siguientes categorías:

- Redes móviles Ad-Hoc.
- Redes inalámbricas de Sensores.
- Redes inalámbricas Híbridas.
- Redes inalámbricas en Malla.

1.6.1 REDES MÓVILES AD HOC

Las redes Ad-Hoc (MANET), se identifican porque los dispositivos (equipos terminales) son nodos móviles. Son redes que no tienen una infraestructura preestablecida pero tienen una topología altamente dinámica, permitiendo que los dispositivos estén libres, es decir se pueden mover aleatoriamente y organizarse arbitrariamente.

La red MANET interconecta a los usuarios permitiendo que éstos intercambien información sin necesidad de tener un punto de coordinación central o acceso (AP). Además, si alguno de los dispositivos tiene un servicio determinado, como el de internet, todos pueden acceder por medio de éste al servicio.

En este tipo de topología, las laptops o dispositivos WiFi de la red inalámbrica que quieren comunicarse entre ellos necesitan usar el mismo canal de radio y configurar un identificar específico de WiFi llamado ESSID en Modo Ad-Hoc.

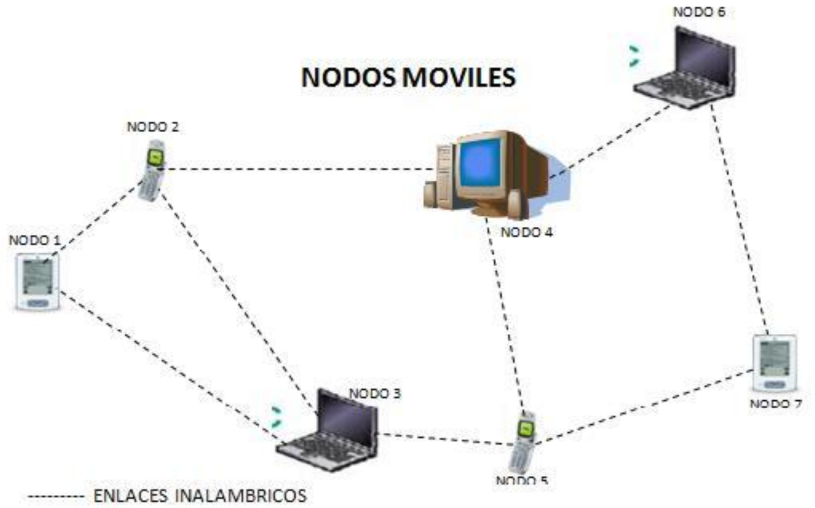


Figura 1-6 Red Móvil Ad-Hoc

1.6.2 REDES INALÁMBRICAS DE SENSORES

Las redes inalámbricas de sensores o WSN se caracterizan por ser formadas por minúsculos nodos sensores espacialmente distribuidos, los cuales permiten recolectar y supervisar parámetros físicos o condiciones ambientales y luego transmitir esta información hacia un nodo de supervisión central.

Los nodos de este tipo de redes tienen el siguiente equipamiento:

- Un Radio Transceiver.
- Un microcontrolador.
- Una batería como fuente de energía.

Las redes WSN inicialmente fueron diseñadas con fines militares, en la actualidad son usadas para solucionar problemas como: supervisión ambiental y del hábitat, control de tráfico, para el cuidado de la salud, automatización casera, entre otras.

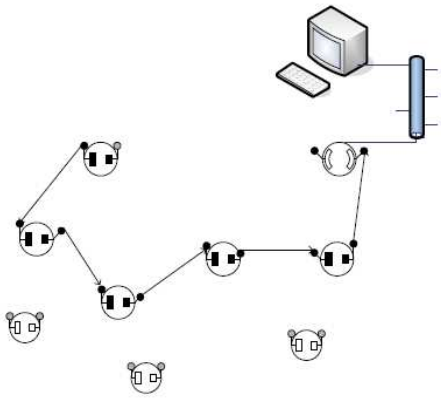


Figura 1-7 Red Inalámbrica Sensorial

1.6.3 REDES INALÁMBRICAS HÍBRIDAS

Una red inalámbrica híbrida o HWN tiene dos componentes principales:

- Una red ad hoc que contiene solo los nodos normales (equipos terminales).
- Una red de estaciones bases.

En este tipo de redes, las estaciones bases están interconectadas por medio de cables de cobre o fibra óptica y son colocadas dentro de la red ad hoc.

Además, las estaciones bases no son fuentes ni receptores de datos a diferencia de los nodos normales, las estaciones solo trabajan como nodos de parada donde se asigna la ruta a los datos para que lleguen a los nodos normales.

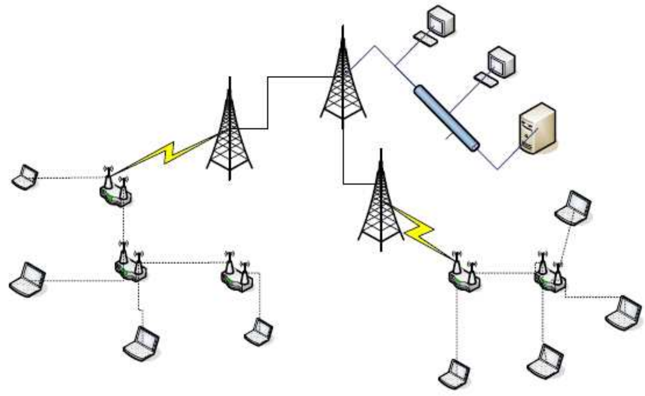


Figura 1-8 Red Inalámbrica Hibrida

1.6.4 REDES INALÁMBRICAS MESH

Las redes inalámbricas en malla o WMN son una tecnología reciente que se está implementando en diversas zonas rurales, urbanas y campus universitarios de Estados Unidos y Europa con resultados exitosos.

Wireless Mesh Network es una variante del WiFi tradicional y una extensión de las redes Ad-Hoc, en la que las clásicas celdas WiFi basadas en cableado Ethernet hasta el switch se sustituyen por una red mallada, donde los nodos se comunican entre sí sin cables, estableciendo una macro-burbuja de cobertura que puede cubrir desde un área pequeña hasta un área relativamente grande.

La red mallada de las WMN permite dar servicios a usuarios móviles, a semejanza de los sistemas celulares. Esta red mallada se crea haciendo la interconexión de celdas de forma inalámbrica utilizando la banda de frecuencias de 5GHz; cada celda puede dar servicio utilizando la banda de frecuencias de 2,4GHz.

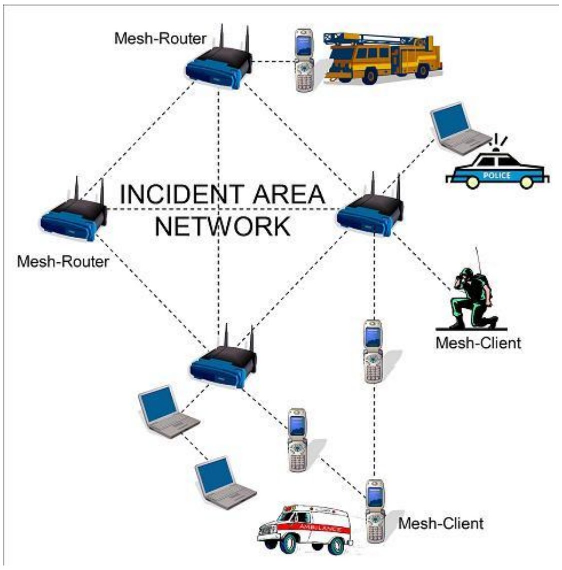


Figura 1-9 Red Inalámbrica en Malla

1.6.5 COMPARACIÓN ENTRE REDES MESH Y AD HOC

Entre las redes inalámbricas en malla y ad hoc existen algunas diferencias, a continuación mencionamos algunas:

- MOVILIDAD:

Las redes Ad Hoc tienen una alta movilidad, mientras que las redes mesh son relativamente estáticas con sus nodos fijos retransmitiendo, por lo tanto las redes WMN tienen una movilidad muy baja en comparación a las MANET.

- TOPOLOGIA:

En las redes MANET la topología de red cambia dinámicamente, mientras que en las redes mesh los nodos permanecen fijos.

- ENERGIA:

En las redes Ad Hoc no se necesita una fuente de energía constante, ya que los equipos terminales o usuarios son laptops, celulares, palms entre otros, los cuales son dispositivos que tienen su propia batería. En las redes mesh debido a que los nodos son estáticos, éstos necesitan estar energizados de manera permanente.

- TIEMPO DE FUNCIONAMENTO DE LA RED:

Las redes mesh después de ser instaladas pueden estar en funcionamiento de forma permanente o hasta que se decida desinstalarlas. Mientras que las redes MANET son temporales.

CAPITULO 2

2. WIRELESS MESH NETWORKS (WMN)

2.1 WIRELESS MESH NETWORKS (WMN)

Las denominadas Wireless Mesh Networks son redes en las que la comunicación se puede hacer entre diferentes nodos y no sólo entre nodo y estación base. Por esta razón son redes descentralizadas, cada nodo es autodirigido y capaz de conectarse a otros nodos como sea necesario.

Estas redes son una combinación de dos topologías inalámbricas, por ello se dice que son una variante del WiFi tradicional (topología infraestructura) y una extensión de las redes Ad-Hoc (topología peer-to-peer).

Las WMN se caracterizan por ser redes autoorganizadas dinámicamente, autoregenerables y autoconfigurables, ya que ellas detectan automáticamente los problemas de ruteo y los solucionan. Además, si se desea extender la cobertura sólo basta con agregar más nodos.

Por las características mencionadas anteriormente las redes mesh permiten tener grandes ventajas como robustez, confiabilidad y un fácil mantenimiento.

2.2 CARACTERÍSTICAS

Las redes malladas tienen características que las diferencian de otras topologías, a continuación nombraremos las principales:

- Las WMN son **redundantes**, los nodos que conforman la red están conectados unos con otros por varios caminos, mediante ésta configuración obtenemos rutas redundantes por todo la red, lo cual permite que si una ruta falla otra se encargará del tráfico de datos.

- **Fácil despliegue,** por ser redes con capacidad de autoconfiguración (routing y selección dinámica de canal), permiten dar soluciones de conectividad en situaciones de emergencia o catástrofes naturales.

- Son **auto-regenerables, auto-configurables**, permiten la **auto-reparación de rutas,** por trabajar con protocolos de última generación mesh, permiten descubrir nuevos nodos admitiéndolos en la comunidad ya existente y regenerando nuevas tablas de encaminamiento.

- Son **robustas,** por el tipo de enrutamiento que se aplica se obtiene una gran estabilidad en cuanto a condiciones variables o en alguna falla de un nodo en particular.

- **Ahorran energía,** para energizar cada nodo de la red mallada no solo se puede usar energía eléctrica sino también energía solar, eólica, hidráulica, celdas de combustible entre otras.

- Su topología permite que sean **útiles en entornos urbanos y rurales,** en los Estados Unidos y en parte de Europa las WMN has sido propuestas para soluciones en entornos urbanos y municipales. Sin embargo, estas redes también son una buena solución para problemas de conectividad en entornos rurales o lejanos.

- **Mayor capacidad a bajo coste**, hay estudios que han demostrado que la capacidad de una red inalámbrica puede ser mejorada mediante la utilización de repetidores [4], existiendo un compromiso entre distancia e interferencia entre nodos.

2.3 SISTEMAS MALLADOS DE PRIMERA, SEGUNDA Y TERCERA GENERACIÓN

Gracias a grandes y medianas empresas que se dedican a desarrollar soluciones de enlaces inalámbricos para la sociedad, los sistemas mallados tienen varias formas de dar servicio y trasmitir datos entre nodos, unos sistemas lo realizan con un solo radio, otros utilizan dos y hasta tres radios. Esto ha provocado que los sistemas mallados se clasifiquen en tres grupos llamados generaciones.

- PRIMERA GENERACION.
- SEGUNDA GENERACION.
- TERCERA GENERACION.

2.3.1 PRIMERA GENERACIÓN

En ésta generación el sistema mallado tiene un solo radio para hacer la interconexión entre nodos y dar servicio, los datos se retransmiten de un nodo a otro de una manera store-and-forward, es decir un nodo primero recibe los datos y luego lo retransmite.

Este sistema tiene desventajas con respecto a los otros, ya que no se puede transmitir y recibir datos simultáneamente por un solo canal de radio porque provocaría interferencia, congestión y contención en cada nodo.

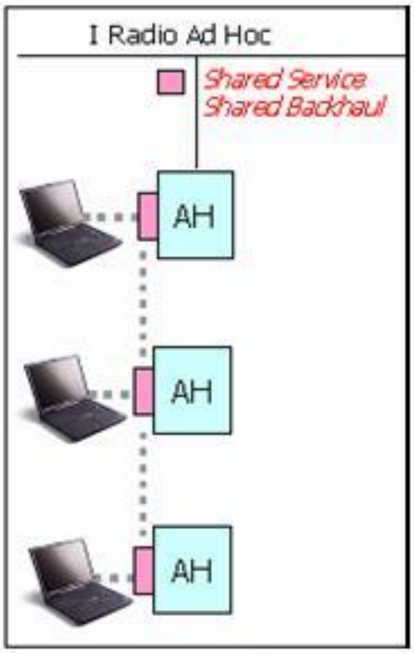


Figura 2-1 Sistema mallado de primera generación

2.3.2 SEGUNDA GENERACIÓN

En esta generación se decidió combinar dos radios, uno para dar servicio con el estándar 802.11b/g y el otro para interconectar los nodos con el estándar 802.11a.

Con este sistema se logró eliminar la interferencia en los nodos ya que se trabaja con diversas bandas de frecuencia (entre 2.4GHz y 5.8GHz) para dar servicio a los usuarios e interconectar nodos, pero se presenta un problema, cuando aumenta la demanda de servicio por parte del usuario se presentan contenciones y congestiones significativas en la parte de la radio que se usa para interconectar los nodos, lo cual hace que este sistema tenga una ligera desventaja.

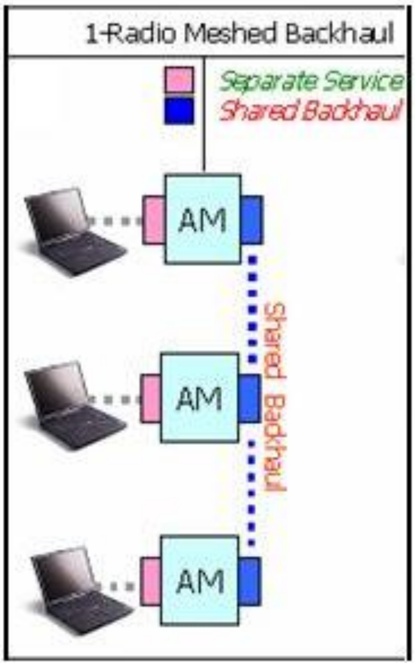


Figura 2-2 Sistema mallado de segunda generación

2.3.3 TERCERA GENERACIÓN

Los equipos de esta generación llevan una gran ventaja en comparación con las generaciones anteriores son considerados equipos inteligentes por utilizar una tecnología moderna, en esta generación cada nodo puede enviar y recibir datos de sus vecinos. Además, los canales disponibles se pueden reutilizar, esto hace que el espectro disponible sea más amplio y que el funcionamiento de la red aumente 50 o más veces.

Las empresas fabricantes de los equipos de esta generación se basan en productos multi-radios que soportan múltiples configuraciones de red.

Un radio de los equipos de tercera generación se usa para crear un enlace hacia su nodo upstream (nodo más cerca al gateway) y otro radio se lo utiliza para un enlace downstream al nodo vecino siguiente. A diferencia de la generación anterior estos radios pueden hacer uso de diversos canales.

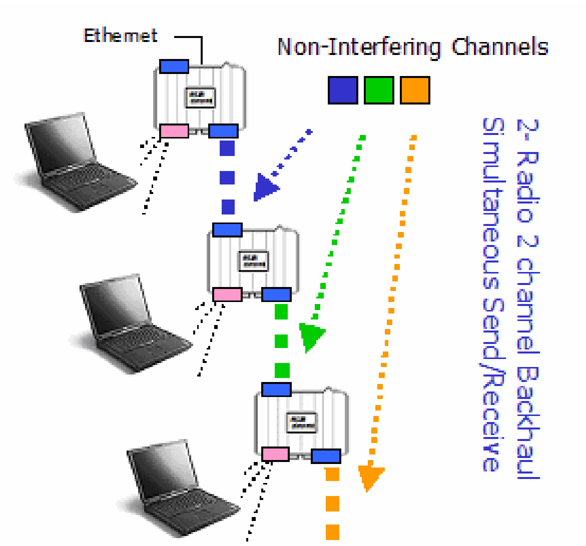


Figura 2-3 Sistema mallado de tercera generación

2.3.4 COMPARACIÓN DE SISTEMAS MALLADOS

La principal diferencia entre los sistemas mallados es el número de radios que utilizan para realizar la interconexión entre nodos (Backhaul) y proporcionar servicio.

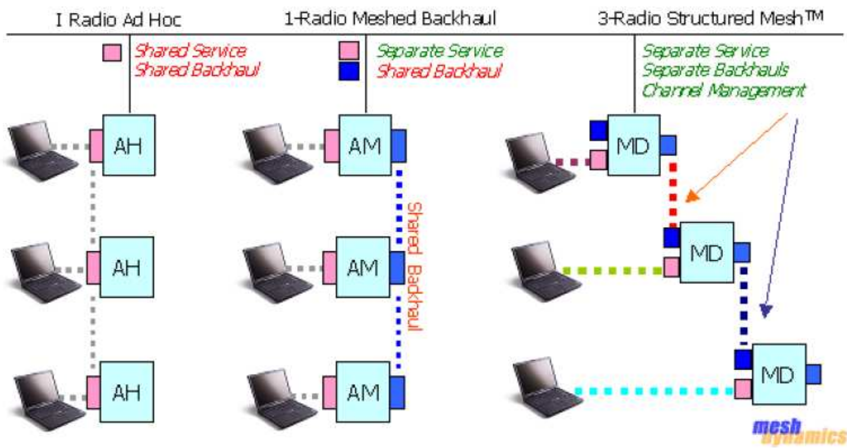


Figura 2-4 Diferencia entre los sistemas mallados

Como se muestra en la figura:

- En la primera generación se utiliza una sola radio, ésta única radio proporciona servicio y backhaul.
- En la segunda generación se utiliza dos radios, en cada nodo se combina un radio con el estándar 802.11b/g para proporcionar servicio y un radio con el estándar 802.11a para interconectar los nodos.
- En la tercera generación se utiliza tres radios, uno para proporcionar servicio y los otros dos radios para

interconectar los nodos, uno para el upstream y el otro para el downstream.

Otro punto a recalcar entre los sistemas mallados, es que no todos los fabricantes de soluciones inalámbricas tienen equipos de las tres generaciones, sino que cada fabricante se ha dedicado a desarrollar y mejorar equipos de una determina generación.

2.4 ARQUITECTURA

La arquitectura de una red inalámbrica mallada tiene dos tipos de nodos, los que trabajan con equipos denominados mesh routers y los que trabajan con equipos denominados mesh clients.

2.4.1 ENRUTADORES MESH

Los enrutadores mesh o mesh routers son equipos que cumplen con el trabajo de un Access Point (AP) convencional, éstos forman una malla de nodos fijos la cual es llamada red de infraestructura o backbone. Además estos equipos pueden trabajar con varias tecnologías de radios para la interconexión entre ellos, como por ejemplo con la IEEE 802.11.

Tienen doble función, el de proporcionar acceso a la red a los clientes y el de hacer una comunicación multi-hop entre ellos para el correcto direccionamiento y entrega de datos.

Figura 2-5 Diferentes modelos de mesh routers.

2.4.2 CLIENTES MESH

Los clientes mesh o mesh clients son dispositivos móviles que tienen la capacidad de conectarse inalámbricamente a una red u otro dispositivo como por ejemplo laptops, celulares, palms, entre otros.

Son los equipos terminales a los cuales se les va a poner a disposición todos los servicios que tiene la red mesh. Además, estos equipos pueden formar una red Ad-Hoc entre ellos, creando una red hibrida con los mesh routers.

Figura 2-6 Equipos Mesh Clients.

2.4.3 CLASIFICACIÓN

Como se ha mencionado en párrafos anteriores la topología en malla se da cuando cada nodo de la red está conectado no solo a otro nodo sino a varios al mismo tiempo, permitiendo llevar datos de un nodo a otro por diferentes caminos.

Tomando como punto de partida este tipo de topología la arquitectura de las WMN puede clasificarse en tres tipos:

- Redes WMN de Infraestructura/Backbone.
- Redes WMN Cliente
- Redes WMN Hibridas.

2.4.3.1 REDES INALÁMBRICAS MESH DE INFRAESTRUCTURA/ BACKBONE

Esta red se forma con un conjunto de mesh routers, la cual va a permitir tener una buena infraestructura para proporcionar servicios a los equipos mesh clients.

La Figura 2-7 muestra como la red que forman los mesh routers sirve de plataforma para que se conecten de forma inalámbrica los mesh clients.

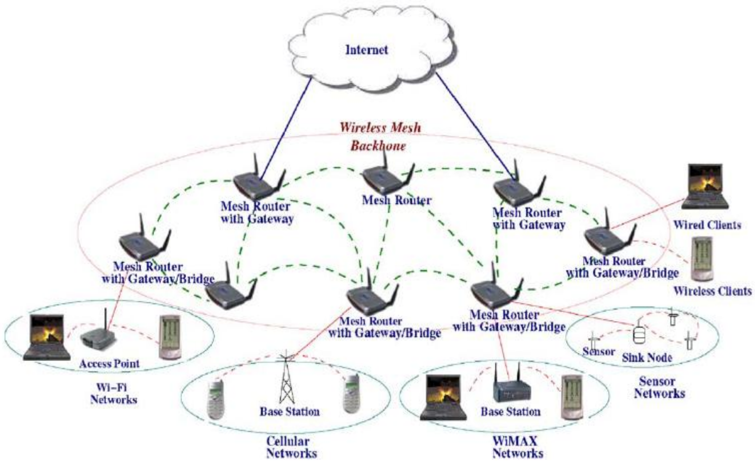


Figura 2-7 Red WMN de Infraestructura

2.4.3.2 REDES INALÁMBRICAS MESH CLIENTE

Esta red está formada por los mesh clientes, los cuales pueden forman una red ad-hoc interconectándose entre ellos de forma peer to peer.

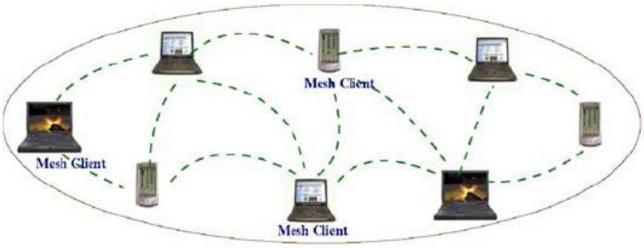


Figura 2-8 Red WMN Cliente.

2.4.3.3 REDES INALÁMBRICAS MESH HIBRIDAS

Es la combinación de las dos redes anteriores, de infraestructura y cliente, es el caso más aplicable al momento de diseñar e implementar una red inalámbrica mallada.

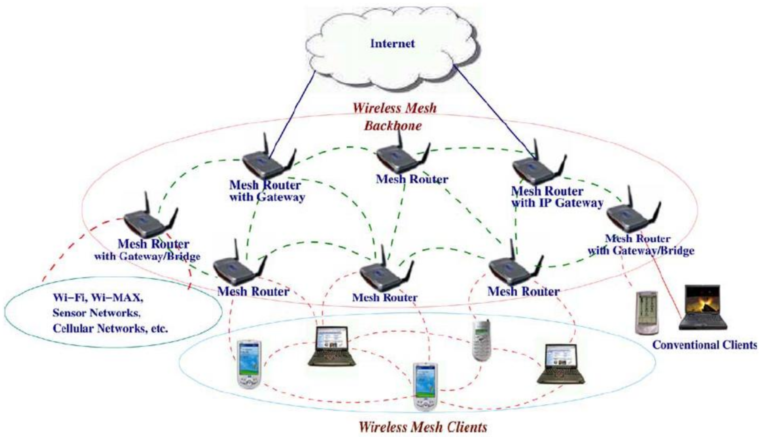


Figura 2-9 Red WMN Hibrida.

2.5 ESTÁNDARES MESH

Los estándares para una tecnología son necesarios ya que estos son los encargados de proporcionar y facilitar la comunicación y la interoperabilidad entre dispositivos de diferentes fabricantes, además permite que el mercado de esta tecnología sea más competitivo, permitiendo a los usuarios tomar decisiones y elegir la mejor opción entre la variedad de productos que tengan los fabricantes.

Existen varios grupos de trabajo que dependiendo del sistema mallado que se desee aplicar y el tipo de servicio que se desea proveer, están trabajando en nuevas especificaciones para las redes malladas o WMN, entre ellos tenemos el IEEE 802.11, IEEE 802.15 y el IEEE 802.16.

2.5.1 IEEE 802.11s

En el primer capítulo se mencionó varios de los estándares de la familia del IEEE 802.11, pero estas normas solo son para comunicaciones one-hop (de un solo salto), por lo tanto no son apropiadas para ser aplicadas en redes multihop (múltiples saltos), multichannel (múltiples canales de transmisión) y cuando se opera con múltiples radios.

Sin embrago, el IEEE creó un grupo de trabajo para que desarrolle el estándar 802.11s para ser usado en redes malladas.

Los equipos que trabajan con el estándar 802.11s, es decir que tienen funcionalidades para trabajar en una red mallada, se denominan Mesh Point (MP). Un sistema de distribución inalámbrico (WDS) es aquel conjunto de MPs conectados en forma de malla. Además en este estándar se involucran equipos como los Mesh Access Point (MAP) y los Mesh Portal Point (MPP) que son MPs específicos, los primeros trabajan como Puntos de Acceso (APs) y los segundos ayudan a interconectar redes malladas.

El estándar 802.11s tiene dos procesos importantes y necesarios para el funcionamiento de una red mallada:

- La asociación de un equipo terminal con un MAP.
- La asociación de un MAP con un nodo vecino.

La función principal del estándar propuesto es realizar la Coordinación del Acceso al Medio denomina MCF, que incluyen procesos como: Aprender la topología de la red mallada, ruteo y forwarding, descubrir topologías y realizar las asociaciones entre nodos, seguridad de la red, configuración y monitoreo.

Cabe mencionar que existen otros estándares que pertenecen al grupo IEEE 802.11 como el 802.11a, 802.11b, 802.11g y 802.11n, que aplicándolos de una manera idónea pueden también trabajar en una red mallada, dando los mismos servicios y aplicaciones como los estándares exclusivos para WMN.

2.5.2 IEEE 802.15

El 802.15 es otro grupo de la IEEE, que está encargado de desarrollar estándares para las Wireless Personal Area Networks (WPANs) o también conocidas como redes inalámbricas de corta distancia.

Las WPANs están orientadas a crear redes inalámbricas con equipos terminales como laptops, PDAs, celulares o cualquier otro dispositivo con tecnología inalámbrica, como se muestra en la Figura 2-10.

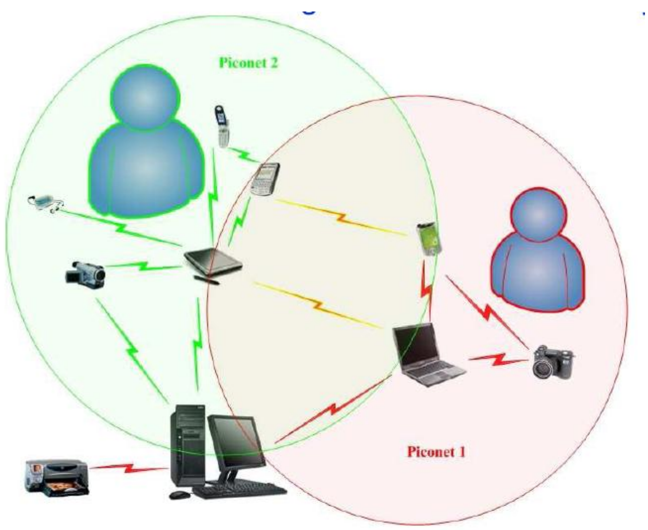


Figura 2-10 Wireless Personal Area Network.

El IEEE 802.15 está dividido en 5 grupos de trabajos, como se muestra en la Tabla II:

Tabla II: Grupos de trabajo del IEEE 802.15

IEEE 802.15 Wireless Personal Area Network (WPAN)		
Grupo de Trabajo	Estándar	Tema
1	802.15.1	WPAN/Bluetooth
2	802.15.2	Coexistencia
3	802.15.3	WPAN High Rate
4	802.15.4	WPAN Low Rate
5	802.15.5	WPAN Mesh

El estándar que se encarga de desarrollar mecanismos para un buen funcionamiento de las capas física y MAC de las WPAN malladas es el IEEE 802.15.5.

Los objetivos de este estándar son:

- Lograr que la cobertura de la red mallada sea amplia.
- Aplicar de forma eficiente las redundancias que existen en las redes malladas.
- Que los mecanismos de autoconfiguración y autoregeneración de rutas sean sencillos.

- Tratar de aumentar la velocidad de conmutación de la información.
- Reducir las retransmisiones.

2.5.3 IEEE 802.16

Los estándares del grupo 802.16 son ideales para ambientes metropolitanos y rurales, porque están diseñados para Broadband Wireless Access (BWA) con un bajo costo de la red y proporcionando alta velocidad de transmisión, facilidad de instalación y gran cobertura.

Entre otras características de estos estándares podemos citar:

- Permiten trabajar en bandas del espectro que necesitan licencia y en las que son libres.
- El servicio que pueden proveer puede ser móvil o fijo.
- Utilizan antenas sectoriales tradicionales o antenas adaptativas con modulaciones flexibles que permiten intercambiar ancho de banda por alcance.

Así como en los grupos de trabajos anteriores el IEEE 802.16 también tiene subgrupos de trabajo, pero el estándar que tiene mecanismos para trabajar en redes malladas es el 802.16a, que tiene las siguientes características:

- Puede trabajar en redes Multihops.
- Opera en el rango de frecuencias bajas 2-11GHz.
- Puede trabajar hasta una tasa de 75 Mbit/s con canales de 20MHz.
- El radio de una celda es de 5 - 10 km aprox.

Además, en las redes que utilizan este estándar se pueden realizar las operaciones de dos maneras diferentes: distribuida ó centralizada.

En la distribuida, todos los nodos deben coordinar con los demás la manera de transmitir para evitar colisiones con los datos y realizar el control de tráfico, también deben enviar por difusión (broadcast) su respectivo estado (recursos disponibles, peticiones y concesiones) a todos sus vecinos.

En la centralizada, los recursos se asignan de una manera más concentrada, ya que la estación base Mesh (dispositivo central de un sector de la red), recopila varias peticiones de un determinado sector y otorga los respectivos recursos para cada enlace, tanto para el downlink como para el uplink, al mismo tiempo que comunica estas decisiones a las demás estaciones bases.

2.6 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento se consideran algoritmos encargados de escoger la mejor ruta que debe seguir un datagrama para llegar a su destino.

El objetivo principal de un protocolo de ruteo en la red inalámbrica Mesh es buscar y establecer una ruta entre los nodos que requieran intercambiar información, es decir seleccionar el camino entre el nodo fuente y el nodo destino.

A continuación se detalla un diagrama de la clasificación de los protocolos de enrutamiento para su mejor compresión:

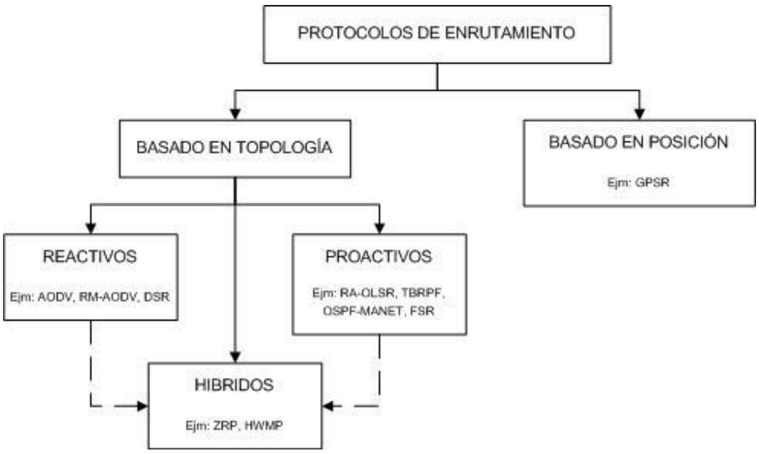


Figura 2-11 Clasificación de Protocolos de enrutamiento en las redes Wireless Mesh

Como se muestra en la Figura 2-11, los protocolos de enrutamiento se clasifican en los dos grandes grupos:

- Protocolos basados en topología.
- Protocolos basados en su posición.

Las redes inalámbricas Mesh pueden trabajar con cualquier tipo de protocolo establecido en la clasificación que se detalló, pero esto no asegura que la red que se desee implementar funcionará correctamente. Escoger el protocolo de enrutamiento adecuado dependerá de algunos factores entre los más importantes están el uso y los requisitos de funcionamiento.

2.6.1 PROTOCOLOS BASADOS EN TOPOLOGIA (TOPOLOGY-BASED)

Este tipo de protocolos de enrutamiento se encargan de seleccionar la trayectoria de los paquetes que van desde un nodo origen a uno de destino basándose en la información topológica.

Los protocolos basados en topología se clasificación en:

- Protocolos Reactivos.
- Protocolos Proactivos.

2.6.1.1 PROTOCOLOS REACTIVOS

También son considerados como protocolos bajo demanda. Estos protocolos determinan las rutas sólo si existe una petición, es decir no intercambian información de manera periódica, evitando una sobrecarga en el ancho de banda debido a que los mensajes de control que se envían a través de la red son mínimos.

El principal inconveniente al utilizar este tipo de enrutamiento es la existencia de retardos al realizar el descubrimiento de rutas, que es el proceso de difundir mensajes de control para que un nodo se pueda comunicar con otro nodo, y éste a su vez le envíe la respuesta de la ruta que se debería seguir.

2.6.1.1.1 AODV

Ad Hoc On-Demand Vector Routing (AODV) es un protocolo de enrutamiento reactivo, como se mencionó los protocolos reactivos están inoperativos hasta que un nodo necesita transmitir un paquete a otro nodo para el cual no tiene ruta, es decir AODV sólo mantiene rutas entre nodos que necesitan comunicarse. Los mensajes únicamente contienen información del los nodos origen y destino, por lo tanto los mensajes de AODV tienen tamaño constante independientemente del número de saltos que existan en la ruta.

BÚSQUEDA POR EXPANSIÓN DE ANILLO.

La búsqueda por expansión de anillo (Expanding-Ring Search) se aplica para descubrir un nodo destino del cual no se conoce ruta alguna. Para lograr su objetivo ésta técnica realiza la difusión de un mensaje que indica cuál es el nodo que se está buscando, pero limitando una zona de rastreo, es decir que no busca ni rastrea todos los nodos de la red.

Si no se logra encontrar al nodo destino dentro del área rastreada, se amplía la zona de exploración para poder repetir el proceso hasta obtener una respuesta por parte del nodo destino, si no es así, se asume que éste nodo es inalcanzable.

DESCUBRIMIENTO DE RUTA

Cuando se desea trasmitir información de un nodo origen a un nodo destino, se genera un procedimiento que se inicia en el nodo origen, el cual envía un mensaje RREQ (paquete de petición de ruta) tipo Broadcast para solicitar la ruta a seguir.

Luego, los nodos vecinos del origen reenvían el paquete RREQ a sus vecinos y así sucesivamente hasta que el RREQ llega a su destino o algún nodo que conozca cómo llegar al destino.

Finalmente cuando se ubica el nodo destino, éste responde con un paquete RREP en unicast.

En la siguiente figura se muestra el proceso completo de envió y recepción de mensajes para el descubrimiento de rutas.

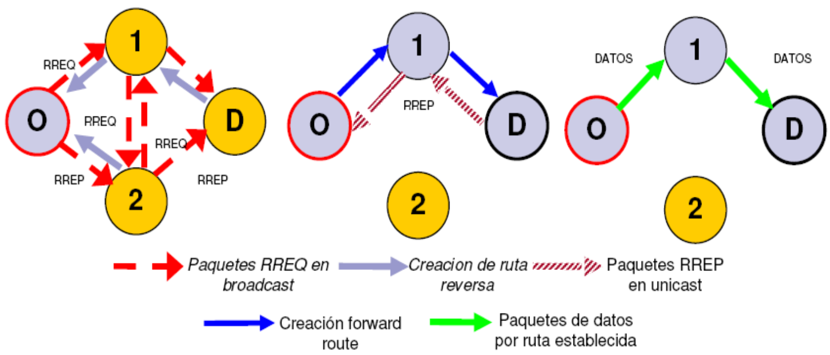


Figura 2-12 Proceso completo de descubrimiento de ruta

MANTENIMIENTO DE RUTA

Cuando un nodo A detecta la pérdida de conectividad con otro nodo B vecino, que es el siguiente salto en una ruta activa, el nodo A procede a difundir un mensaje de error

RERR a sus vecinos, el cual contiene la dirección IP del nodo B, es decir el nodo que está alarmado y se lo considera como nodo “inalcanzable”.

Cuando otro nodo C recibe un mensaje RERR, éste busca en su tabla de enrutamiento si tiene registrado al nodo B que se ha convertido en inalcanzable; si esta ruta existe, entonces es invalidada y el nodo C procede a difundir un nuevo mensaje RERR a sus vecinos. Este proceso continúa hasta que el nodo fuente recibe el mensaje RERR, entonces éste procede a invalidar las rutas registradas y reinicia un nuevo proceso de descubrimiento de ruta.

Cuando un nodo se desconecta y reconecta por el motivo que sea, perderá el número de secuencia y los números de recuento de las rutas hacia sus destinos, pudiendo provocar bucles en el enlace. Lo que hace el nodo al reiniciar es vaciar la tabla de rutas y evita contestar los RREQ durante un tiempo definido por DELETE_PERIOD, que es tiempo necesario para vaciar la tabla de encaminamiento.

FORMATO DEL MENSAJE RREQ

El mensaje RREQ se envía para solicitar una ruta hacia un determinado nodo destino.

El formato de este mensaje es el siguiente:

Tabla III:Formato del mensaje RREQ del protocolo AODV

0	8					13	24 31
Tipo	J	R	G	D	U	Reservado	Cuenta de Saltos
RREQ ID							
Dirección IP Destino							
Número de Secuencia Destino							
Dirección IP Fuente							
Número de Secuencia Fuente							

FORMATO DEL MENSAJE RREP

El mensaje RREP se envía como contestación a un RREQ confirmando un establecimiento de ruta. Sigue el formato siguiente:

Tabla IV: Formato del mensaje RREP del protocolo AODV

0	8	9	10	19	24 31
Tipo	R	A	Reservado	Tamaño de Prefijo	Cuenta de Saltos
Dirección IP Destino					
Número de Secuencia Destino					
Dirección IP Fuente					
Tiempo de Vida					

FORMATO DEL MENSAJE RERR

En la siguiente figura se muestra el formato del mensaje RERR.

Tabla V: Formato del mensaje RERR del protocolo AODV

0	8	9	24 31
Tipo	N	Reservado	Cuenta Destino
Dirección IP Destino Inalcanzable			
Número de Secuencia Destino Inalcanzable			
Dirección IP Destino Inalcanzable Adicional			
Número de Secuencia Destino Inalcanzable Adicional			

2.6.1.1.2 DSR

El Protocolo de Enrutamiento de Fuente Dinámica o Dynamic Source Routing (DSR) es un protocolo de enrutamiento sencillo y eficiente que permite a la red ser completamente auto-organizada y auto-configurable.

Para poder realizar el encaminamiento, en el lado del nodo origen a cada paquete de datos se le inserta una cabecera DSR de opciones que se colocará entre la cabecera de transporte y la dirección IP, donde se incluirá la ruta que debe seguir el paquete desde el nodo fuente hasta el nodo destino.

DSR permite múltiples rutas a cualquier destino y también que cada remitente pueda seleccionar y controlar las rutas a utilizar en el enrutamiento de sus paquetes, como para su utilización en el “balanceo de carga” o para aumentar la robustez de la red.

El protocolo DSR se compone de dos mecanismos importantes: "Descubrimiento de Rutas" o “Route Discovery” y "Mantenimiento de Rutas" o “Route Maintenance”, que trabajan juntos para permitir que los nodos puedan descubrir y mantener las rutas a destinos arbitrarios dentro de la red.

Este protocolo opera totalmente bajo demanda, es decir que si la red sufre algún cambio, DSR reaccionará automáticamente cambiando las rutas para poder trabajar sin problemas.

2.6.1.2 PROTOCOLOS PROACTIVOS

Los protocolos proactivos se encargan de establecer todas las rutas posibles dentro de la red Mesh, por lo que el intercambio de mensajes de control se lo realiza periódicamente.

La búsqueda de rutas en la red es de manera inmediata, ya que se encontrarán continuamente actualizadas, pero a su vez ocasiona sobrecarga en el ancho de banda debido al número de peticiones que se realizan, disminuyendo la capacidad de la aplicación de los usuarios.

2.6.1.2.1 OLSR

Optimized Link State Routing Protocol (OLSR) es un protocolo que utiliza mensajes “Hello” y mensajes de control de topología (TC) para descubrir las rutas y así discriminar información del Enlace de Estado. Los nodos que son independientes usan esta información de topología para calcular los siguientes saltos para todos los nodos de la red, debido a que utilizan el salto más corto para la transmisión de caminos.

Este protocolo utiliza el concepto de la transmisión multipunto o Multipoint Relay (MPR) con el objetivo de reducir una sobrecarga por la retransmisión de paquetes tipo Broadcast, además de reducir el tamaño de los paquetes del enlace de Estado (LS).

De forma resumida, los vecinos de un salto del nodo A son las trasmisiones multipunto MPR del mencionado nodo, de tal manera que cada vecino de doble salto del nodo A pasa a ser un vecino de un salto de al menos un nodo MPR identificado para el nodo A. Lo mencionado se puede identificar en la figura que se presenta a continuación:

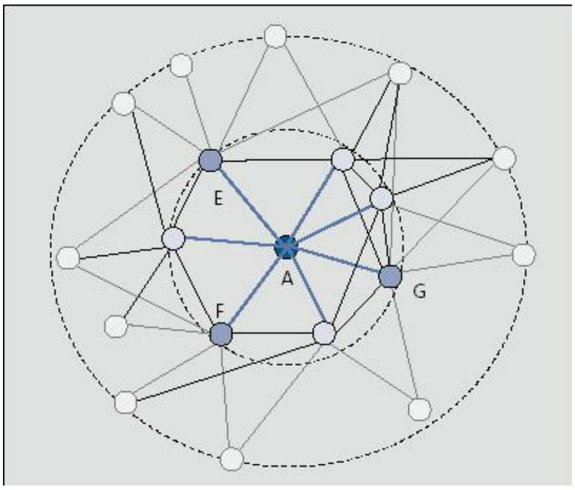


Figura 2-13 Ilustración de los MPRs en OLSR

Donde, los nodos E, F y G son nodos vecinos de un salto o nodos MPRs del nodo A y los que están en la parte limitante de la red son nodos doble salto del nodo A.

2.6.1.2.2 TBRPF

Topology Dissemination Based on Reverse-Path Forwarding es un protocolo de Enlace de Estado que proporciona enrutamiento salto a salto (hop-by-hop) a lo largo de caminos más cortos para cada destino.

En este protocolo cada nodo calcula un árbol fuente proporcionando siempre caminos para llegar a todos los nodos, basándose en la información de la topología parcial que se almacena en la tabla de topología de cada nodo, para lo cual se utiliza el algoritmo de Dijkstra.

Para minimizar el consumo de ancho de banda en la red, cada nodo informa parte de su árbol a todos sus vecinos, realizando actualizaciones periódicas y diferenciales para mantener informados a todos sus vecinos de la información del árbol que posee.

2.6.1.2.3 HSLS

El protocolo Hazy-Sighted Link State Routing Protocol (HSLS), se basa en un algoritmo que permite a las computadoras comunicarse a través de la radio digital de una red Mesh que transmite mensajes a los equipos que están fuera del alcance directo.

HSLS se hizo para que funcione muy bien en redes que cuentan con más de 1000 nodos, teniendo mejores resultados sobre otros algoritmos de enrutamiento. Esto se logra mediante un equilibrio cuidadosamente diseñado de actualización de frecuencia y métrica, con el fin de propagar la información del enlace de estado de manera óptima. HSLS no inunda la red con información del enlace de estado para hacer frente a los nodos móviles que cambian las conexiones con el resto de la red. Además no requiere que cada nodo tenga la misma vista de la red.

2.6.1.2.4 MMRP

EL Protocolo de Enrutamiento Móvil Mesh o Mobile Mesh Routing Protocol funciona de tal manera que los nodos periódicamente emiten un datagrama UDP conocido como LSP (Paquete de Estado de Enlace) sobre cada interfaz de todos los nodos de la red en modo broadcast. MMRP divide sus procesos en protocolos, los cuales tienen funciones específicas detalladas en la siguiente tabla:

Tabla VI: Protocolos del MMRP

LINK DISCOVERY	Descubre enlaces-protocolo HELLO
ROUTING-LINK	Verifica el estado del enlace
BORDER DISCOVERY	Activa túneles externos

2.6.1.2.5 OSPF

Open Short Path First (OSPF), fue desarrollado por la IETF con la especificación RFC 2328. Es un protocolo que surgió como alternativa del protocolo RIP que se basa en el enlace de estado o algoritmo Short Path First.

A continuación se enuncian varias características importantes del OSPF:

Implementa el algoritmo de Dijkstra para calcular la ruta más corta a cada red de destino.

Ruteo de múltiples trayectorias de costo basado en ToS (Type of Services).

Calcula rutas separadas para cada tipo de servicio IP. Varias rutas para un destino.

Emplea multicast en vez de broadcast, para reducir la carga en los sistemas que no emplean OSPF.

Informa sobre las interfaces disponibles, métrica utilizada y otras variables enviando anuncios LSAs (Link State Advertisements).

2.6.1.3 PROTOCOLOS HÍBRIDOS

Un ejemplo de protocolo híbrido es el Hybrid Wireless Mesh Protocol (HWMP) el cual surge como una alternativa de los protocolos de enrutamiento basados en topología ya que según las características de la red puede ser modificada de manera dinámica, es decir que en caso de que existan redes pequeñas y estáticas, lo más idóneo es utilizar protocolos proactivos, pero si la red es todo lo contrario, es decir una red grande y con movilidad lo mejor es utilizar protocolos reactivos.

Así, con la combinación de rutas bajo demanda y protocolos proactivos se lograra tener una enrutamiento de red robusto ya que se obtendrá flexibilidad para la creación de redes mesh donde los nodos son móviles y reducir la carga de trafico de control intra-mesh en redes con nodos fijos.

2.6.2 PROTOCOLOS BASADOS EN POSICIÓN

Los protocolos de enrutamiento que se basan en la posición se encargan de seleccionar las trayectorias tomando en cuenta la información geográfica empleando algoritmos geométricos. La posición del nodo destino se la va a obtener por medio de un servicio denominado Location Service.

El algoritmo empleado es el Greedy Forwanding, que es un algoritmo simple de búsqueda donde el paquete que se envía se lo manda hacia el nodo vecino que está más cercano del nodo destino, aunque trate de acercarse a su destino no asegura que lo pueda alcanzar aunque haya un enlace definido.

La gráfica muestra un modelo sobre este tipo de protocolo, donde también se identifica las técnicas que se emplean para la búsqueda de la trayectoria que se detallarán a continuación:

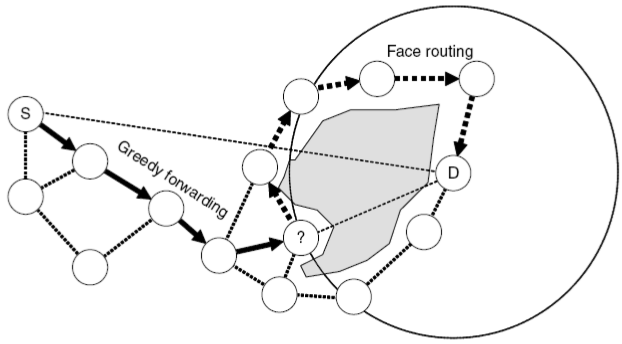


Figura 2-14 Expedición basada en posición

2.6.2.1 FACE ROUTING

Face Routing es una estrategia que se utiliza para segmentar la red de manera lógica (no se cruzan los enlaces) como se muestra en la Figura 2-15, para lo cual se emplean algoritmos distribuidos.

También es conocida como Encaminamiento en Faceta, o como Regla de la Mano Derecha (Right-Hand Rule).

Además, emplea la técnica de vector distancia para seguir el camino más corto, simple y sin la presencia de bucles.

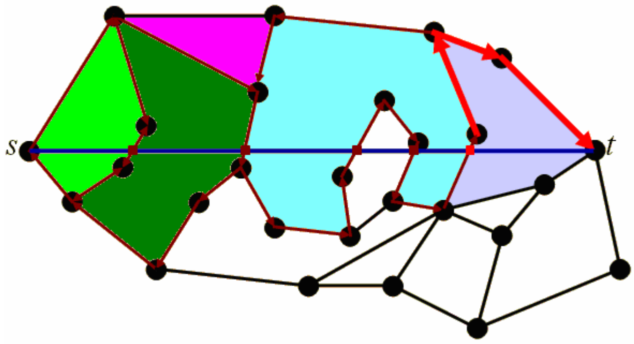


Figura 2-15 Encaminamiento en grafos planos mediante Face Routing

2.6.2.2 GPSR

Greedy Perimeter Stateless Routing (GPSR) es el protocolo basado en posición más conocido en lo que respecta a redes inalámbricas. El procedimiento de este tipo de enrutamiento se basa en aplicar el concepto del Greedy Forwarding en conjunto con técnica de Face Routing.

El algoritmo que emplea GPSR es distinto a los algoritmos de ruteo 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 geográficas en una red inalámbrica, usando las posiciones de nodos para tomar decisiones con respecto al forwarding(traslado) de los paquetes.

Los beneficios de esta técnica radican que un nodo sólo tiene que recordar la información de localización de los nodos vecinos que se encuentran a un salto, para lo cual aplica la transmisión de paquetes por medio del Piggybacking, permitiendo que las decisiones de enrutamiento puedan ser realizadas de manera dinámica.

2.7 CAPAS DEL MODELO OSI EN LAS REDES MESH

2.7.1 CAPA FÍSICA

En las redes mesh por poseer una gran densidad de nodos y un espectro radio eléctrico limitado, para un perfecto funcionamiento de éstas, es necesario optimizar el uso de los canales minimizando las interferencias. Los mecanismos básicos para lograr dicha minimización de interferencia son:

- Selección Dinámica de Frecuencia o DFS.
- Control de Potencia o TPC.

Estos mecanismos al ser aplicados a las redes WMN necesitan de un buen control por parte de los protocolos de capas superiores.

Para aumentar la eficiencia espectral se utiliza la técnica MIMO (Multiple Input Multiple Output), con esta técnica se logra capacidades superiores a los 108 Mbps en el enlace inalámbrico.

En las WMN no solo se puede aplicar una tecnología de radio, sino que puede aplicarse varias, en función de la capacidad y cobertura deseada éstas pueden ser:

- Ultra Wide Band o UWB.
- Orthogonal Frequency Division Multiplex u OFDM.

En la actualidad se están desarrollando investigaciones de tecnologías y protocolos para la capa física que se orientan a mejorar la capacidad ofrecida por las redes WMN, como por ejemplo; utilización de antenas inteligentes, antenas adaptativas o de antenas auto configurable y reprogramables vía software.

2.7.2 CAPA MAC O DE CONTROL DE ACCESO AL MEDIO

La capa MAC en las WMN trata de solucionar los problemas del nodo oculto y nodo expuesto en las redes multisaltos, existen mecanismos que ayudan a solventar este problema como por ejemplo TDMA (Time Division Multiple Access) que es muy útil siempre y cuando exista una buena sincronización del sistema.

Para problemas como el de la interferencia, existe un mecanismo denominado CDMA (Code Division Multiple Access), este mecanismo puede disminuir los efectos de las interferencias, ya que dos nodos pueden ocupar simultáneamente un solo canal empleando códigos distintos.

Los protocolos de la capa MAC se pueden dividir en dos categorías:

- Protocolos basados en contención.
- Protocolos basados en libres colisiones de los canales.

Que los protocolos se basen **en contención,** significa que éstos consideran que no hay entidad central que asigne los canales en la red, es decir que para que un nodo transmita debe tener su propio medio. Pero esto tiene su desventaja, ya que cuando más de un nodo trata de transmitir al mismo tiempo van a existir colisiones.

Los protocolos basados en contención incluyen Aloha, CSMA y CSMA/CA.

Aloha transmite conforme le van llegando los paquetes, si más de un nodo tiene paquetes por transmitir, éstos colisionan y se destruyen por la falta de sincronización.

CSMA (Acceso Múltiple por Detección de Portadora), sensa si existe portadoras en el canal que se va a trasmitir, si esta libre envía toda la trama, si no espera un pequeño intervalo de tiempo para retransmitir.

CSMA/CA (acceso múltiple por detección de portadora con evasión de colisiones), cuando un nodo tiene información para transmitir anuncia su intención antes de hacerlo para evitar colisiones. Así los nodos vecinos sabrán que el canal no está disponible y esperaran un tiempo aleatorio corto para utilizarlo. Las redes inalámbricas 802.11 utilizan el **CSMA/CA.**

Los protocolos que se basan en una **libre colisión de los canales** se caracterizan porque asignan canales dedicados a cada nodo que desea trasmitir, este mecanismo lo utilizan el TDMA, CDMA y FDMA teniendo como ventaja la eliminación de colisiones con eficiencia.

TDMA (Acceso múltiple por división de tiempo), es considerado como una tecnología inalámbrica de segunda generación, ya que distribuye las unidades de información que se desean transmitir en ranuras alternas de tiempo llamadas slots, con esto se logra dar acceso múltiple a un número reducido de frecuencias. Una de las principales características de este protocolo es que permite dar servicios de voz y datos con una alta calidad.

CDMA (acceso múltiple por división de código), se basa en el espectro expandido o ensanchado, es decir la información se extiende sobre un ancho de banda significativamente mayor que el original, dicha información se trasmite como una señal codificada de manera que se pueda trasmitir junto atrás señales emitidas por nodos vecinos usando el mismo medio.

FDMA (Acceso múltiple por división de frecuencia), consiste en dividir el espectro disponible en canales, que corresponden a distintos rangos de frecuencia, dichos canales se los asignan a cada uno de los nodos para que puedan transmitir.

En la actualidad existe una gran demanda por equipos con el estándar 802.11 de la IEEE por su bajo coste, por ello se convierten en una solución atractiva para implementar redes multi-salto. Es por esto que existen propuestas de protocolos a nivel de MAC para las redes 802.11 basados en distintos objetivos de diseño. Cabe recalcar que la IEEE en el estándar

802.11s incluye mecanismos de enrutamiento a nivel de la capa 2 y un acceso al medio más eficiente.

La capa Mac, además de controlar el acceso al medio puede controlar la utilización de canales simultáneamente, mediante propuestas como MMAC y HMCP, al igual como lo realizan capas superiores, obteniendo como resultado una mejor capacidad de la red.

MMAC (Multichannel MAC), trabaja con varios canales de radio con solo una sola interfaz de radio, por esta razón se necesita una buena señalización y coordinación para que todos los nodos escuchen el canal adecuado en cada momento.

HMCP (Hybrib Multichannel Protocol), trabajan con nodos que tienen varias interfaces de radio, unas trabajan en canales fijos y otras en canales variables.

2.7.3 CAPA DE RED

Los protocolos de enrutamiento de la capa de red son los encargados de darle a las redes malladas las características de auto-configurables y auto reparables, es por ello que dichos protocolos deben cumplir con las siguientes características:

Métrica de funcionamiento múltiple

Para que los paquetes que se envíen lleven una trayectoria adecuada y no existan perdidas.

Escalabilidad

Los protocolos usados en WMN deben perdurar en el tiempo y a la vez ser accesibles a mejoras.

Robustez

Ya que las redes malladas deben de ser estables, es decir no se debe interrumpir el servicio de la red por alguna eventualidad de ésta, como por ejemplo la falla en un nodo en particular. Además se debe evitar la congestión de la red para ello se utiliza el balanceo de carga.

Infraestructura Mesh con ruteo eficiente

Con la infraestructura tipo malla de los routers se puede lograr que el ruteo hasta el usuario de la red sea simple, así la interconexión entre usuario y red será eficiente.

Existen varios protocolos de enrutamiento que se han desarrollado para las WMN, pero de acuerdo a las características mencionadas se recomienda el uso de MANET (Mobile Ad-Hoc Networks) del IETF, el cual se divide en protocolos reactivos con el AODV (Ad-Hoc Ondemand Distance vector) y proactivos con el OLSR (Optimizad Link State Routing).

Además si en la red los Routers mesh no tienen mucha movilidad y sus rutas no varían tan dinámicamente, se puede utilizar el protocolo OSPF (Open Shortest Path First) con su extensión de movilidad para que permita la autoconfiguración de la red en el caso de que se pierda conexión con algún nodo.

MÉTRICAS EN REDES MALLADAS

Las métricas que utilizan los protocolos de enrutamiento deben de garantizar QoS en la red, para lograr esto las métricas deben proporcionar información sobre el estado del enlace y así poder seleccionar la mejor ruta para llegar al destino.

Existen varias propuestas en cuanto a las métricas, entre ellas tenemos:

ETX o Expected Transmission Count, que permite realizar una estimación del número de retransmisiones necesarias por enlace.

ETT o Expected Transmission Time, que estima el tiempo de transmisión de cada paquete de datos.

WCETT o Weighted Comulative ETT, empleando distintos canales con distintas capacidades se puede seleccionar el mejor enlace en cada momento.

2.7.4 CAPA DE TRANSPORTE

Protocolos para la capa de transporte en la WMN no se han propuesto, pero existen protocolos como el TCP (Transport Control Protocol) que es el más usado en la actualidad en redes de datos basadas en IP, y puede ser implementado aunque tenga sus desventajas en las redes inalámbricas.

El protocolo TCP clásico supone que las pérdidas de paquetes se dan por la congestión que existe en los nodos, lo cual es una de las desventajas que existe cuando se desee aplicar este protocolo en las WMN ya que si las pérdidas se dan por algún otro factor ajeno a la congestión, éste puede hacer que el rendimiento de la red disminuya.

Por lo mencionado se recomienda que para las redes malladas se debería aplicar variantes o mejoras del protocolo TCP, o simplemente proponer nuevos protocolos, que permitan optimizar el transporte en las WMN.

2.7.5 CAPA DE APLICACIÓN

Las WMN son redes que pueden proveer muchos servicios a los usuarios, entre ellos tenemos:

TENER UNA RED MESH COMUNITARIA.

Implica mejorar el estilo de vida de las personas que habitan en una comunidad o en áreas donde exista una población numerosa, permitiéndoles tener aplicaciones como:

- Acceso a Internet compartido.
- Vigilancia y seguridad vecinal (videocámaras).
- Compartición de contenidos multimedia (vecindad de DVRs).
- Respuesta médica y de emergencia.
- “eBay vecinal” (venta y mercadillo).
- Tablón de anuncios virtual.

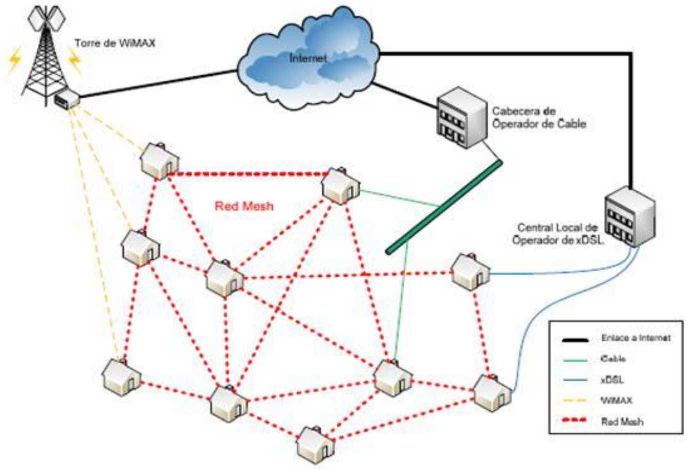


Figura 2-16 Red mesh comunitaria.

<u>TENER UNA RED MESH MUNICIPAL</u>.

Implica implementar en las zonas comerciales de una ciudad una red, donde se permita modelos de negocios como por ejemplo administrar un negocio con varias sucursales desde un solo punto.

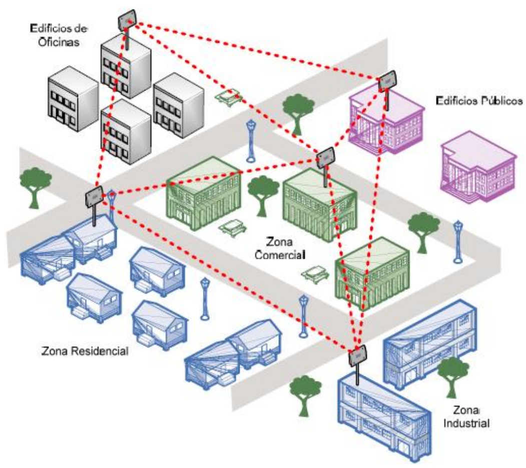


Figura 2-17 Red mesh municipal.

TENER UN HOGAR MESH.

Implica que los dispositivos que tengan tecnología inalámbrica en el hogar puedan ser descubiertos y ser integrados en una sola red. Entre los dispositivos que tienen esta tecnología tenemos:

- Equipos de audio y vídeo.
- Teléfonos móviles y fijos.
- Laptops, Palms.
- Interruptores inteligentes, sistemas de inteligencia ambiental.

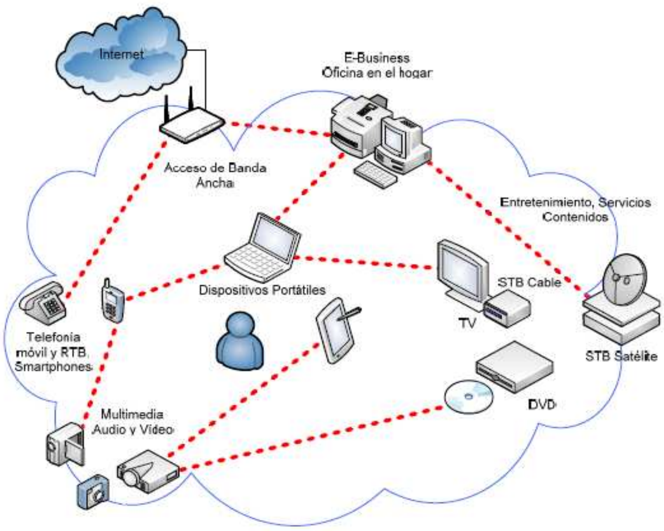


Figura 2-18 Hogar mesh.

TENER UNA RED MESH ESPONTÁNEA.

Implica tener un sistema donde nos permita obtener servicios de voz, video y datos. Un ejemplo de esto es que se podrían realizar llamadas peer-to-peer.

TENER UN CAMPUS MESH.

Implica proveer servicios de comunicación a universidades o instituciones educativas. En la actualidad es el servicio más solicitado de las redes malladas, ya que lo podemos ver en grandes universidades de Estados Unidos y Europa.

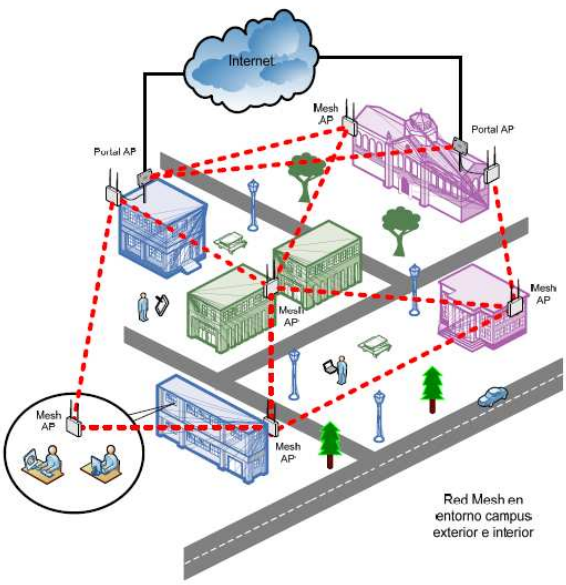


Figura 2-19 Campus mesh.

2.8 CALIDAD DE SERVICIO (QoS) EN LAS REDES MESH

En los últimos años el despliegue de las redes Mesh ha sido visto como un prometedor paso hacia el objetivo de tener un acceso inalámbrico de banda ancha en cualquier lugar y a cualquier horario. La Calidad de Servicio QoS es una cuestión crítica, especialmente en las redes empresariales y redes troncales, que dependen de la provisión de un adecuado soporte QoS cuando se ha desplegado una red mesh.

Debido a la naturaleza del broadcast en el medio inalámbrico, las redes inalámbricas necesitan darle importancia a problemas como el de la interferencia y el ruido, lo cual no es un problema en redes cableadas. En contraste con la tradicional red celular de un solo salto (single-hop), las redes multi-hop como las redes ad-hoc y las redes Mesh introducen otros factores que enfatizan en el problema de la interferencia, por ejemplo el simple hecho de que una ruta multi-hop necesita más transmisiones comparada a una conexión de un salto single-hop, podría generar ruido.

2.8.1 ESCENARIOS DE APLICACIONES DE REDES MESH

Los mecanismos para un soporte de QoS en una red Mesh pueden ser diseñados e implementados teniendo en cuenta los siguientes escenarios:

- Escenario Corporativo o Empresarial
- Escenario Operador/Proveedor
- Escenario Usuario Final

ESCENARIO CORPORATIVO (EMPRESARIAL):

En este escenario las redes Mesh son desplegadas por una organización para servir como un troncal de banda ancha inalámbrica proporcionando servicios de backhaul. Ejemplos de estas redes inalámbricas son redes troncales de un campus universitario, o para una organización.

Además, tal troncal de banda ancha inalámbrica de la red Mesh puede ser desplegado a fin de responder en caso de desastres o emergencias. En este caso, la red WMN proporciona la infraestructura para la comunicación entre los diferentes equipos de rescate, que se comunicarían a través de dispositivos inalámbricos de usuarios como por ejemplo un hand-held.

La red WMN es responsable del soporte QoS para habilitar varios servicios, que puede ser usado para facilitar la comunicación punto a punto y la transferencia de datos útil para controlar de forma remota actuadores tales como robots que se han desplegado en áreas de riesgo.

El soporte de QoS en estos escenarios de aplicación es fundamental debido a que las aplicaciones tienen tiempos de respuesta estrictos, así como requerimientos de ancho de banda.

ESCENARIO OPERADOR / PROVEEDOR:

Las redes Mesh son una interesante alternativa para los proveedores de red que deseen ampliar la cobertura de su infraestructura de red existente, sin incurrir en una planificación exorbitante y costos elevados.

Las zonas rurales sin conectividad pueden contar con una red inalámbrica de banda ancha con cobertura de una red Mesh. Los usuarios pueden utilizar el servicio triple-play (voz, datos y video) a través de una red inalámbrica, además de ofrecer movilidad de los abonados. Los mecanismos aplicados permiten el soporte a nivel de carrier-grade en VoIP, e incluso videoconferencia, video streaming y juegos en línea multiusuario. Por lo tanto, el proveedor está interesado en mecanismos de QoS que permiten la diferenciación de los múltiples servicios en la infraestructura de una red Mesh.

ESCENARIO USUARIO FINAL:

En las comunidades, las redes Mesh se construyen generalmente utilizando equipos cliente-operador, que crecen en una manera no planificada. Estas redes son una alternativa más barata a las redes tradicionales cableadas para los usuarios.

En las zonas que carecen de una amplia infraestructura de red, estas redes son vitales para proporcionar acceso a Internet a comunidades enteras, a pesar de que sólo uno o unos pocos nodos funcionen para dar acceso directo a Internet. Dichas redes podrán ser destinadas para uso de aplicaciones P2P entre vecinos, servicios de administración y de servicio a la comunidad.

La mayoría de las aplicaciones en este escenario no tienen estrictos límites por retardos de enlace pero si tienen beneficios cuando tienen un gran ancho de banda disponible. La calidad de servicio se mide por la optimización de la capacidad de uso, el control que se realiza cuando el tráfico está saturado y la calidad del tráfico de voz. Además, se considera un punto muy importante la seguridad de la red ante amenazas externas.

2.8.2 CONSIDERACIONES EN LAS REDES MESH

La calidad de servicio (QoS) en el estándar IEEE 802.16 se basa en el principio de comunicación de paquete-por-paquete utilizando partes del identificador de conexión en malla (Mesh CID) presente en el Protocolo de Unidad de Datos (PDU) de la capa MAC para decidir la manipulación por salto del paquete. Además, el identificador Mesh CID se utiliza para especificar si un paquete necesita ser transmitido en caso de que se haya perdido.

El mecanismo mencionado es válido siempre y cuando se considere tener un ancho de banda suficiente para los distintos enlaces de la red Mesh, para ello se utiliza las tecnologías TDMA / TDD con la reutilización espacial para asignar ancho de banda a los distintos enlaces y compartir el ancho de banda disponible entre los diferentes nodos.

Cabe mencionar que el estándar 802.16 es compatible con los siguientes mecanismos de asignación de ancho de banda en el modo Mesh:

1. Programación Coordinada Centralizada

2. Programación Coordinada Distribuida

3. Programación No Coordinada Distribuida

PROGRAMACIÓN COORDINADA CENTRALIZADA

Las asignaciones de ancho de banda se gestionan de forma centralizada por la estación base (BS) Mesh. La estación base específica una programación en diagrama de árbol que toma como inicio o raíz del árbol a la estación base.

PROGRAMACIÓN COORDINADA DISTRIBUIDA

Los nodos programan sus transmisiones hasta sus vecinos de dos saltos de tal manera que las transmisiones no tengan conflictos. Los nodos utilizan un protocolo handshake de tres vías (solicitud, confirmación, reconfirmación) para reservar de ancho de banda para un enlace.

PROGRAMACIÓN NO COORDINADA DISTRIBUIDA

Los nodos usan los mismos mecanismos que en la Programación Coordinada Distribuida con excepción del algoritmo de elección Mesh. Los mensajes handshake no se transmiten en la subtrama de control pero si en la subtrama de datos. La transmisión de mensajes se lleva a cabo en minislots ya reservados para los enlaces en cuestión (por ejemplo, el enlace de un nodo de transmisión de datos hacia el nodo de recepción de datos y viceversa).

2.8.3 DESAFÍOS, RETOS Y SOLUCIONES

En esta sección se presentan soluciones de QoS basadas en hipótesis, donde se utilizan los requisitos por encima de los escenarios y se considera estandarizar tecnologías de las redes Mesh como un marco para las soluciones de QoS. Además se abordan desafíos de la vida real (incluyendo los aspectos de implementación) como el paso siguiente para hacer del QoS-aware de las redes Mesh una realidad.

DIFERENCIACIÓN DEL SERVICIO, INTERWORKING

Para permitir varias aplicaciones, la diferenciación del servicio es fundamental. El estándar IEEE 802.16 define para el modo de operación Punto-Multipunto (PMP) los siguientes servicios:

- Unsolicited Grant Service (UGS)
- Real-Time Polling Service (rtPS)
- Non real-Time Polling Service (nrtPS)
- Best Effort: Mejor Esfuerzo(BE)

Para cumplir con los servicios mencionados se debe diseñar una buena arquitectura de QoS y desarrollar mecanismos para soportar sofisticados servicios de programación, considerando:

PROVISIÓN DE QOS END-TO-END

Mecanismos de QoS por enlace y por salto. Para el soporte de QoS a nivel de portador es necesario direccionar un régimen end-to-end dentro de la red Mesh.

GESTIÓN DE ANCHO DE BANDA ADAPTABLE E EFICIENTE

En una red Mesh cuando diferentes clases de tráfico son compatibles, la reservación de ancho de banda tiene que adaptarse a las necesidades de las aplicaciones.

VALORES ÓPTIMOS DE LOS PARÁMETROS DEL ESTÁNDAR

El modo Mesh implica varios protocolos de estado y parámetros que deben ser optimizados ya que la elección de los parámetros para la distribución mediante el algoritmo de elección Mesh influye en el rendimiento de la red y ocasionan un retardo en el handshake de tres vías para establecer el ancho de banda. Además, se debe tener en cuenta estándares para la operación de las redes, crecimiento de toda la red, parámetros de auto-adaptación en caso de que un nodo falle y quede fuera de servicio.

CUESTIONES DE FIABILIDAD Y SEGURIDAD

La seguridad inalámbrica es muy importante en especial si es una red no planificada que crece constantemente, por lo que aspectos como la fiabilidad deben ser abordados. Protocolos de auto-estabilización en conjunto con mecanismos de gestión de cada uno de los nodos de la red desempeñan un papel fundamental.

MOVILIDAD Y CAPA FÍSICA

Funciones como soporte de movilidad o mecanismos para la capa física tales como el uso concurrente de múltiples canales inalámbricos, antenas dirigidas añaden complejidad al problema.

Esto origina la necesidad de encontrar soluciones que permitan el interworking y la compatibilidad entre los estándares que son viables para una red Mesh estática de backhaul y la tecnología para apoyar la movilidad de los usuarios.

2.9 SEGURIDAD EN LAS REDES MESH

2.9.1 TECNOLOGÍA UTILIZADA PARA LA SEGURIDAD

Las redes inalámbricas Mesh se exponen a las mismas amenazas a las que están sometidas las redes cableadas y otras tecnologías inalámbricas, como mensajes interceptados, modificados, retrasados, reenviados o insertados. Lo que se busca es que el usuario tenga la mayor privacidad posible, en la que incluye anonimato, seudonimidad y confidencialidad de tráfico. Los servicios de seguridad que se tratan de asegurar y proteger son:

Confidencialidad: Los datos son revelados sólo en las entidades o personas interesadas.

Autentificación: Una entidad tiene de hecho la identidad que demanda tener, es decir, reconocimiento de los usuarios dueños del servicio.

Control de acceso: Se asegura de que solo acciones autorizadas puedan ser realizadas.

No negación: Protege las entidades que participan en un intercambio de información.

Disponibilidad: Se asegura de que las acciones autorizadas puedan tomar lugar.

La protección del tráfico de comunicación implica la confidencialidad (cifrado), la autenticación, protección de la integridad y de la autenticidad de mensajes intercambiados.

Puede ser protegido en diversas capas como: capa de enlace, capa de red, capa de transporte y capa de aplicación, que incluyen medios para proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, protocolos de autentificación y algoritmos criptográficos.

Las redes inalámbricas WLAN se apoyan en dos modos de seguridad que son el acceso WPA (Acceso de Protección al Wifi) y la versión más actualizada WPA2, además de incluir un cifrado compartido configurado en los dispositivos como el cifrado precompartido PSK donde los usuarios pueden ser autenticados con un servidor denominado server AAA. Para este propósito, se utiliza el protocolo extensible de autenticación EAP (Extensible Authentication Protocol).

La autenticación ocurre entre la estación móvil (MS) y el servidor AAA usando EAP al como se ve en la Figura 2-20. EAP es transportado entre el MS y el punto de acceso (AP) y entre el AP y el servidor AAA a través de la autentificación del RADIUS. Si es habilitado el nodo, una sesión de cifrado maestra (MSK) es utilizada, el cual se envía desde el servidor de autenticación al punto de acceso AP.

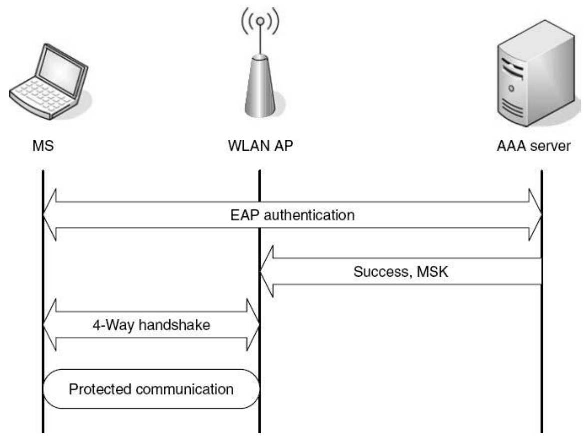


Figura 2-20 Acceso a WLAN basada en EAP

Hay cuatro maneras que establecen una sesión de cifrado temporal para proteger el enlace inalámbrico. Este cifrado se utiliza realmente para proteger el tráfico del usuario, usando cualquier protocolo dominante temporal de la integridad (WPA) o AES-basado en CCMP (WPA2). Los varios métodos de EAP que existen para una autenticación se basan en los certificados digitales, las contraseñas, o los protocolos móviles de reuso de la autenticación de la red (EAP-SIM, EAP-AKA).

El tráfico de la comunicación se puede también proteger en la capa de enlace. Un aspecto fundamental en la seguridad es el protocolo IPsec que se encarga de proteger el tráfico IP en la capa de la red. La arquitectura de IPsec especifica dos protocolos de seguridad: Encapsulation Security Payload (ESP) y Authentication Header (AH). En el caso del protocolo ESP, solo encapsula la carga útil (payload) del paquete en modo transporte o como un paquete IP completo (incluyendo cabecera) en el caso que sea modo del túnel. Una IPsec Security Association (SA) define las llaves (keys) y los algoritmos criptográficos para utilizar. Una Asociación de Seguridad SA es identificada por tres aspectos consistentes en: una dirección IP destino, un protocolo identificador (AH o ESP) y un índice del parámetro de la seguridad.

El protocolo IPsec es usado regularmente en redes privadas virtuales (VPN) para tener acceso con seguridad a la Intranet de una compañía. El tráfico de la comunicación se puede proteger en la capa de transporte usando el protocolo de seguridad TLS. Su uso principal está para proteger el protocolo Http sobre TLS/SSL (https), pero esta puede también ser utilizada como protocolo independiente.

Es también posible proteger el tráfico en capas de mayor nivel, lo cual permitirá realizar operaciones y aplicaciones específicas de seguridad. Por ejemplo, los E-mails pueden ser encriptados (protección a la confidencialidad) y/o ser señalados aplicando autentificación e integridad para que solo le llegue al destino.

2.9.2 DESAFÍOS PARA LA SEGURIDAD MESH

Los desafíos para la seguridad de las redes Mesh se basan en sus características topológicas.

Comparando las redes malladas con otras tecnologías se puede mencionar como desafío de seguridad, el mejorar la confiabilidad de la red en la comunicación de múltiples saltos.

El Multihopping es necesario para que la red mallada amplíe su cobertura sin que sea importante tener línea de vista (LOS) entre los usuarios, ya que retrasa la detección y el tratamiento de los ataques, hace encaminar un servicio de red crítico y los nodos confían en otros nodos para comunicarse. Mientras que el uso de enlaces inalámbricos hace una red mesh susceptible a los ataques, la exposición física de los nodos permite que un adversario tome, clone, o trate de forzar a estos dispositivos.

Otros desafíos específicos para las redes Mesh son:

- Las redes pueden ser dinámicas debido a cambios en su topología y a la frecuencia con que los nodos entran y salgan de la red. Por lo tanto, ninguna seguridad con configuración estática sería suficiente.

- Los routers y clientes mesh llevan a cabo características muy diversas tales como la movilidad y la energía. Consecuentemente, la misma solución de la seguridad no puede trabajar para ambas al mismo tiempo para un router mesh y un cliente mesh.

2.9.3 ATAQUES POTENCIALES EN LAS REDES MESH

Hay dos fuentes de amenazas en este tipo de redes inalámbricas: Ataques Externos y Ataques Internos.

Los atacantes externos son puestos en marcha por intrusos que no pertenecen a la red mesh y tratan de acceder ilegítimamente a la red, donde pueden atorar la comunicación o inyectar una información errónea. Los principales ataques se basan en la encriptación y autenticación.

Los ataques internos son aquellos que provienen de nodos que forman parte de la red, estas amenazas son más severas, puesto que los ataques internos no son tan fáciles de prevenir como los externos, debido a que tienen acceso a toda la manipulación de información y autenticación de la misma.

Existen Mecanismos de cooperación que ayudan a detectar y aislar los nodos conocidos como mecanismos de “mal comportamiento” o misbehaving que necesitan ser empleados.

Podemos identificar ataques pasivos que se proponen a robar la información y espiar en la comunicación dentro de la red, y ataques activos donde el atacante modifica e inyecta paquetes en la red.

Los ataques podrían apuntar a varias capas de protocolos. En la capa física, un atacante puede embotellar las transmisiones de antenas inalámbricas o simplemente destruir el hardware de cierto nodo. Tales ataques se pueden detectar y localizar fácilmente.

En la capa MAC, un atacante puede enviar paquetes de control y de datos a nodos que pertenecen a la red o personificar un nodo legal. Aquí podemos distinguir los siguientes ataques:

Eavesdropping: En este ataque se guarda una copia de la información de los datos, a su vez que lidera el compromiso en la confidencialidad y la integridad de los datos.

Ataque de Jamming: Los nodos malévolos se encargan de transmitir las cabeceras de las tramas de la capa MAC sin carga útil (payload) en el canal de transmisión. Aquí se producen ataques que son causados por Flooding, es decir, que los nodos se sobrecargan. Ataques más avanzados se basan en mensajes de gestión de protocolo inteligente que tratan de forzar. También se produce agotamiento de energía de los nodos legítimos.

Ataque de Suplantación (Spoofing): Se aplica Eavesdrop en la red Mesh para determinar las direcciones MAC de los dispositivos legítimos y poder enmascararse como un usuario legítimo. Se produce la Denegación de Servicio DoS o el acceso ilegal.

Ataque de Repetición: El intruso produce una copia o aplica Eavesdrop a los datos entre dos nodos y transmiten los mensajes legítimos en una etapa posterior para hacerse pasar como un usuario legítimo.

Un atacante podía también explotar los protocolos de la capa de red, en la cual se clasifica en ataques del Plano de Datos (Data Plane) y ataques del Plano de Control (Control Plane).

En lo que respecta a los ataques del Plano de Datos conocemos que por lo general se ponen en marcha por nodos “egoístas” o nodos “maliciosos” con la finalidad de hacer “caer” los paquetes o inyectar de datos maliciosos. El objetivo de un atacante es causar la denegación de servicio (DoS) a los usuarios legítimos haciendo que los datos de los usuarios no se puedan entregar.

Los ataques del Plano de Control tienen como objetivo la funcionalidad del enrutamiento de la capa de Red. El propósito de un atacante es convertir las rutas en inaceptables o controlar el camino del enrutamiento. Estos ataques a su vez se clasifican en:

Ataque Apresurado (Rushing): Propiciado por un nodo malicioso que envía el mensaje de solicitud de ruta (Route Request) antes que cualquier otro nodo intermedio especificado, haciendo caso omiso de la demora (delay) especificada.

Ataque de Agujero de Gusano (Wormhole): Un ataque procura convencer a nodos que utilicen una trayectoria malévola formada por dos nodos maliciosos en convivencia entre sí que forman un túnel que es considerado como un medio de comunicación eficaz y legítimo. Un adversario con capacidades rápidas de búsqueda puede remitir rápidamente un mensaje con un acoplamiento bajo del estado latente.

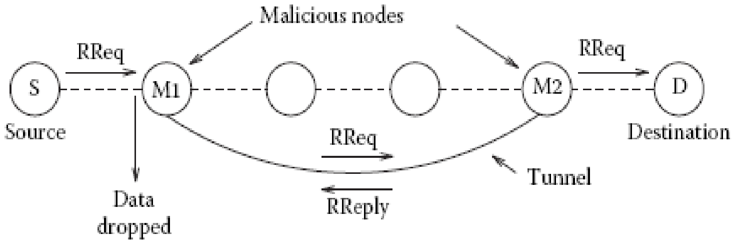


Figura 2-21 Ataque Wormhole

Ataque del Hoyo Negro (Blackhole): El nodo malicioso siempre responde de manera positiva a la petición de ruta (Route Request) aunque no pueda tener una ruta válida hacia el destino. Casi todo el tráfico de los nodos vecinos al nodo malicioso se orientarán hacia él y se "caerán" todos los paquetes.

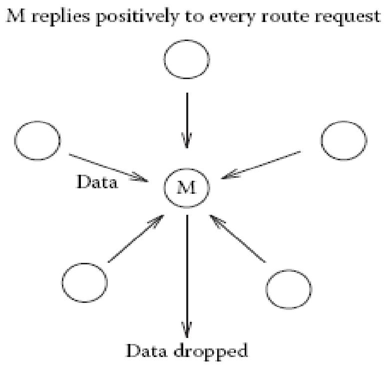


Figura 2-22 Ataque Blackhole

Otro tipo es el de packet forwarding o transmisión del paquete, es decir, el atacante puede no cambiar las tablas de ruteo, pero los paquetes en la trayectoria de enrutamiento pueden ser conducidos a diferentes destinos que no sean consistentes con el protocolo de enrutamiento. Por otra parte, el atacante puede esconderse en la red y personificar un nodo legítimo que no sigue las especificaciones requeridas de un protocolo de encaminamiento. En la capa de aplicación un atacante podía inyectar una información falsa o imitada, dañando la integridad de su uso.

2.9.4 MECANISMOS DE SOLUCIÓN DE SEGURIDAD DE UNA RED MESH

Para prevenir la presencia de ataques de nodos intrusos, una red inalámbrica Mesh debe tener la capacidad de desempeñar dos funciones muy importantes como son la prevención y detección de intrusos.

En lo que se enfoca a la prevención de intrusos deben existir servicios de seguridad que impiden que el atacante ingrese y ataque a la red. Esta prevención incluye la autenticación, control de acceso, confidencialidad e integridad de datos.

Para la detección de intrusos se deben identificar las actividades ilícitas, los cuales son consecuencias de un ataque o que pueda conducir a un ataque.

La mayoría de los mecanismos de seguridad y protocolos aplican el enfoque de prevención. A continuación se detallan como diferentes servicios de seguridad encajan en el modelo de seguridad de una red inalámbrica Mesh:

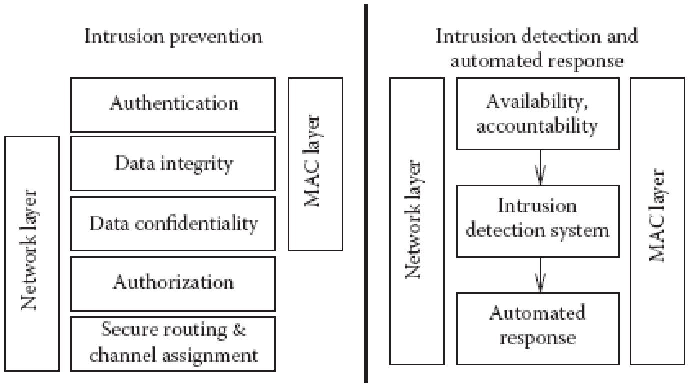


Figura 2-23 Prevención y detección de intrusos

Dentro de los mecanismos de seguridad de las Redes Mesh podemos identificar lo siguiente:

- Mecanismo del Establecimiento de Firme Confianza en contra de conductas de nodos egoístas y maliciosos dentro de la red.

- Diferenciar entre un router Mesh y un cliente Mesh para poder identificar los requisitos de seguridad y las limitaciones.

- Servicios de seguridad End-to-end con el fin de contrarrestar el comportamiento egoísta y malicioso de nodos enrutados para que la red Mesh facilite servicios de seguridad end-to-end, además de una base por enlace.

- Rendición de cuentas para garantizar el comportamiento de los nodos de acuerdo a la especificación del protocolo, incluso si los nodos tomen sus decisiones independientemente acerca de enrutamiento y asignación del canal.

Una posible solución a la autenticación tiene como primer punto tener en cuenta una clave pública criptográfica para autenticación de routers Mesh, y así obtener una menor limitación de recursos, que estará firme a ataques internos. Para este recurso se hará uso de una función de una vía para llevar a cabo la autenticación con clave pública en lugar de una Certificación de Autoridad (CA).

La aplicación del Modelo de Autenticación Dual para la autenticación de clientes Mesh autorizados se debe realizar durante el proceso de Roaming, es decir cuando se cambia de un router inalámbrico Mesh a otro.

En lo que se refiere a la Autenticación de los routers Mesh, la idea básica consiste en que cada router Mesh tenga un certificado de un par de claves publica/privada asignadas por la entidad administrativa, para lo cual cada router antes de desplegarse con todas las claves públicas de los routers de la red no requiere recurrir a un Certificado de Autoridad (CA). Para la revocación o la adición de nuevos nodos se las realiza mediante Broadcast.

Con la finalidad de prevenir el ataque del Plano de Control de la capa de Red hay que tener en cuenta el Enrutamiento Multicamino, el cual nos proporciona caminos alternos entre el origen y el destino cuando ocurran los ataques, aumentando el rendimiento ya que se trabaja con los mecanismos de detección de intrusos. Además, al garantizar los protocolos de enrutamiento, se obliga a cada uno de los nodos para seguir el protocolo de enrutamiento.

Otro protocolo que emplea seguridad es SAODV, que aplica la utilización de firmas digitales para autenticar todos los campos de los mensajes de petición de ruta Route Request y respuesta de ruta Route Reply.

Para la solución de un enrutamiento seguro podemos establecer los siguientes puntos:

- Relación de protocolos Proactivos vs Reactivos

- Autenticación del Remitente
- Autenticación de la Información de Enrutamiento

2.10 PROGRAMACIÓN DE EQUIDAD Y BALANCEO DE CARGA

En este punto se detallará el funcionamiento de la Programación de Equidad o Fair Scheduling que se ofrece para la red inalámbrica Mesh, así como la importancia de aplicar el balanceo de carga en la red para la utilización de los múltiples enlaces con la finalidad de evitar congestión y saturación de tráfico.

2.10.1 PROGRAMACIÓN DE EQUIDAD

En una red Mesh sólo un hostspot (HS) está conectado a Internet, el resto de la red está compuesta por puntos de acceso transientes (TAPs) que usan la comunicación inalámbrica para la transferencia del tráfico de sus clientes desde y hacia hotspot (HS). Sin embargo esta red está sujeta a sufrir interferencia lo que ocasiona un gran problema para la transmisión y recepción de datos de los usuarios, por lo que al planificar una programación de equidad, aseguramos dos aspectos muy importantes que son:

- Asegurar la equidad Fairness para cada cliente.

- Optimizar la utilización de ancho de banda en la red Mesh.

La solución para que una transmisión sea eficiente es utilizar en los enlaces la tecnología STDMA o Spatial TDMA, ya que TDMA (Acceso Múltiple por División de Tiempo) no puede activar dos enlaces al mismo tiempo, en cambio STDMA si lo puede realizar siempre y cuando no estén mutuamente sostenidos, permitiendo que la red sea libre de colisiones sin importar que exista un tráfico elevado en el flujo de datos.

2.10.2 CLASIFICACIÓN DE LA PROGRAMACIÓN (SCHEDULING)

Para realizar la siguiente clasificación hay que basarse en el rendimiento Throughput y la equidad Fairness:

MÁXIMO THROUGHPUT SCHEDULING:

Optimiza la utilización del recurso pero ocurre un “starvation” si hay varios flujos transmitiéndose simultáneamente con diferentes costos, donde la alta prioridad de al menos un flujo “costoso” cierra el paso de tráfico de un flujo pequeño.

FAIRNESS IGUAL / MEJOR ESFUERZO:

Dentro del punto de equidad Fairness los usuarios que emplean “Greedy” con un gran flujo son favorecidas sobre flujos más pequeños a pesar de tener asignados los mismos intervalos de tiempo para cada flujo.

EQUIDAD MAX-MIN (ENCOLAMIENTO EQUITATIVO):

La tasa de datos mínima son maximizadas para cada flujo resultando un rendimiento alto como el caso del Fairness Igual, pero a pesar de los cambios sigue siendo mucho menor que el rendimiento máximo.

FAIRNESS PROPORCIONAL:

Se utilizan prioridades y funciones de peso para maximizar el rendimiento al mismo tiempo que se proporciona la mínima calidad de servicio QoS.

2.10.3 BALANCEO DE CARGA

Se conoce que uno de los beneficios de este tipo de redes es la redundancia de camino múltiple. Sin embargo algunas veces muchos nodos utilizan los mismos enlaces causando congestión mientras otros enlaces están inactivos. Muchos consideran al Balanceo de Carga como un método que permite lograr equidad en una red Mesh.

El método de Balanceo de Carga puede ser aplicado:

- En los enlaces
- En los routers Mesh
- En las Puertas de Enlace (Gateways) hacia el Internet
- Por partición de la red

La distribución de tráfico de una red Mesh es desigual, donde la mayoría de los nodos de una red Mesh se comunican con nodos de una red cableada. El objetivo del Balanceo de Carga es ayudar a evitar enlaces con cuello de botella (bottlenecks) e incrementar la eficiencia de la utilización de los recursos de la red.

El enrutamiento del Balanceo de Carga se basa en la construcción de un árbol básico de manera similar como se utiliza el algoritmo de formación Spanning Tree pero recalcando que la métrica utilizada por cada nodo para determinar el nodo padre es dinámica para lograr el balanceo de carga.

Para realizar la métrica al enrutamiento lo primero que se realiza es el contador de saltos (Hop Count) que resulta ser más estable ya que es más estático, además que se produce de manera rápida la convergencia. También tenemos la capacidad residual del Gateway, en la cual tenemos más carga balanceada, así como también la red se adapta al tráfico y las rutas tienen menos intermitencias debido a que la red es dinámica. Finalmente tenemos la capacidad residual del camino donde debido al peso y flujo del tráfico los enlaces se modifican evitando cuellos de botella en el Gateway.

Al asignar el canal tenemos un punto conocido como la Conexión al Interface del Vecino, en la cual el problema en el diseño de un algoritmo de asignación de un canal distribuido es la dependencia del canal entre los nodos. También tenemos la Asignación de la Interface del Canal, donde para asignar canales se necesita estimar un aproximado del estado de uso de todos los canales dentro de la interferencia de todos los nodos de la red.

2.10.3.1 BALANCEO DE CARGA DEFINIDO

Balanceo de carga es una característica deseable para tener en un despliegue de la red inalámbrica Mesh , ya que reduce la congestión en la red, aumenta el rendimiento de red, y evita la interrupción del servicio en caso de avería. El balanceo de carga se puede definir en las dos formas siguientes:

BALANCEO DE CARGA POR RUTA:

El balanceo de carga por ruta puede mejorar el rendimiento de la red y la fiabilidad mediante la distribución de tráfico entre un conjunto de diversos caminos.

El balanceo de carga por ruta proporciona una insignificante mejora del rendimiento en redes inalámbricas Multi-hop, porque la ruta de acoplamiento es un resultado de la proximidad geográfica de caminos aspirantes. Esto puede conducir a la auto-interferencia entre estos caminos y, por tanto, repercutir negativamente en el rendimiento.

BALANCEO DE CARGA BASADO EN SU GATEWAY:

En esta interpretación de balanceo de carga, el tráfico se distribuye entre un conjunto de gateways en la red Mesh, es decir una de las varias puertas de enlace es elegida como el punto de salida de los flujos procedentes de la red.

La mejora del rendimiento balanceo de carga basado en su Gateway será mayor que con el balanceo de carga por ruta, porque la ruta de acoplamiento a diferentes puertas de enlace de un punto final en red Mesh se espera que sea menor en un despliegue bien planificado. Por esta razón, la arquitectura MeshCluster soporta balanceo de carga basado en su puerta de enlace.

2.10.3.2 PROTOCOLO DE BALANCEO DE CARGA BASADO EN SU GATEWAY

Un punto de acceso se encuentra en los árboles que corresponden a las puertas de enlace de la red. Ese punto de acceso selecciona uno de los Gateways descubiertos como su puerta de enlace predeterminada. El Gateway predeterminado es por el cual el punto de acceso puede lograr la más alta capacidad (según lo determinado por la métrica de enrutamiento). El punto de acceso típicamente utiliza este Gateway predeterminado como punto de salida para todos los flujos que se han iniciado a través de él.

Cada punto de acceso en la red también monitorea la calidad del mejor camino a cada uno de sus puertas de enlace. El mejor camino es simplemente el camino en el árbol Spanning Tree calculado para aquel Gateway.

La calidad de la ruta es monitoreada utilizando una herramienta de prueba conocida como el tiempo de viaje de ida y vuelta (RTT).

La herramienta reporta los valores RTT para cada uno de los Gateways en la red. El gateway con el “menor retardo” se designa como el Gateway de “menor carga”. En una red Mesh sin carga, el Gateway predeterminado suele ser el Gateway de “menor carga”. Cuando un punto de acceso detecta que su Gateway predeterminado suele ser diferente que el Gateway de “menor carga” se deduce que hay congestión en el camino que conduce a su puerta de enlace. En este caso, todos los flujos iniciados por los puntos de acceso utilizan el Gateway de “menor carga” como su punto de salida.

El punto de acceso no migra cualquiera de sus existentes flujos al Gateway de “menor carga”. Esto es necesario en cualquier despliegue Mesh que hace traducción de direcciones de red NAT en los Gateways, de lo contrario el flujo de migración puede dar lugar a la interrupción a menos que el estado por flujo en el NAT también sea migrado. Por lo tanto, evitamos que se realice la migración de los actuales flujos, el cual puede estar en “stand by” en caso de que no sea necesario realizar un NAT para poder tener salida hacia el Internet.

La migración de los flujos al Gateway de “menor carga” puede originar intermitencias en la ruta que ocurren cuando varios flujos migran al Gateway de “menor carga” y resulta que el Gateway se convirtió previamente en una puerta de enlace sin carga. Los puntos de acceso detectan el cambio y comenzar a utilizar el Gateway original como punto de salida. El cambio que se produce hace que el segundo Gateway se convierta en un Gateway sin carga.

Para mitigar intermitencias en los enlaces se colocan administradores de arbitraje en cada puerta de los enlaces, ya que estarían pendientes de las solicitudes de flujo de migración y por ende migrarían los flujos de manera inteligente.

2.11 ASPECTOS IMPORTANTES A CONSIDERAR EN LAS REDES INALÁMBRICAS MESH

En esta sección se discuten aspectos importantes que deben tenerse en cuenta en las Redes Inalámbricas Mesh, tales como la capacidad, la imparcialidad o mejor conocido como Fairness, la fiabilidad, la solidez, y la gestión de los recursos.

2.11.1 CAPACIDAD DEL RENDIMIENTO

En los sistemas de comunicación de datos y telecomunicaciones, el rendimiento o mejor conocido como Throughput se define como el número de bits o caracteres (datos) por unidad de tiempo que se distribuyen sobre un medio cableado o inalámbrico. Como un ejemplo, podemos decir que el rendimiento o Throughput es la cantidad de datos por segundo que pasan a través de un cable de conexión entre dos ordenadores, o la información que se transmite en un medio inalámbrico entre dos nodos. Entonces, la capacidad total de la red es el máximo rendimiento (throughput) de un nodo o enlace de comunicación.

La capacidad del rendimiento Throughput también puede definirse como el máximo rendimiento posible λ con una elevada probabilidad (asintóticamente aproximado a 1), donde λ es la tasa de llegada en bits por segundo, y cada nodo de la red envía los datos con una alta probabilidad a su destino elegido.

En las redes inalámbricas Mesh, una de sus grandes limitaciones es el rendimiento. El límite superior teórico de la capacidad del rendimiento de cada nodo es limitado asintóticamente por $\theta(1/\sqrt{n})$ donde *n* es el número de nodos en la red. Por lo tanto, al aumentar del número de nodos, la capacidad del Throughput por nodo se convierte en inaceptable por su baja capacidad.

En general, el Throughput aceptable en una red Mesh es proporcional a $\theta(W \times n^{-1/d})$ donde *d* es la dimensión de la red, y *W* es el ancho de banda total. Un enfoque para mejorar la capacidad del Throughput es el uso de múltiples radios y de protocolos adecuados.

Los nodos tienen mejor rendimiento Throughput en un sistema de un solo canal (single-channel) que en un sistema multicanal (multi-channel). Además, existen otros factores que contribuyen a la degradación del rendimiento Throuhput tales como características en la MAC, el problema de terminal oculto, el problema de un nodo expuesto, y la tasa de error en el canal inalámbrico los cuales tienen más efecto en un sistema de un solo canal.

2.11.2 GESTIÓN DE RECURSOS

La gestión de los recursos se encarga del manejo eficiente de los recursos de la red como son: la energía, el ancho de banda, interfaces y el almacenamiento.

Por ejemplo, si tenemos un nodo con dos interfaces, un nodo con baja potencia y otro nodo regular, entonces la red Mesh puede utilizar de manera eficiente los recursos energéticos. En general, el consumo de energía, incluso en modo de espera, depende mucho del tipo de la interface. Por lo tanto, basándose en el estándar IEEE 802.11, una red Mesh con reserva de energía limitada, una red con baja potencia y una interface con baja tasa de transmisión de datos puede ser utilizada para llevar información de señalización out-of-band para controlar la alta potencia y la interface con alta tasa de transmisión de datos.

Los recursos de ancho de banda también se pueden gestionar mejor en un entorno multiradio. Por ejemplo, el balanceo de carga cruza a través de múltiples interfaces para evitar que un canal se encuentre muy congestionado, se forme un posible cuello de botella (Bottleneck) y por tanto produzca saturación y lentitud en el servicio de la red. Además, el ancho de banda de cada interface puede ser agregado para obtener una alta tasa efectiva de datos. Por último, un mecanismo de agregación de ancho de banda y una programación de paquetes dinámicos se pueden utilizar para obtener un mejor rendimiento.

2.11.3 EQUIDAD

Equidad o Fairness es un término que se refiere al compartimiento de ancho de banda de múltiples nodos a través del enlace de tránsito de manera simultánea, sin priorizar preferencia alguna por algún nodo, evitando el problema de interferencia cuando varios desean transmitir hacia un mismo destino.

Los nodos de un solo radio (single-channel) de alto rendimiento también se enfrentan a la falta de una distribución equitativa. La red tiene un Fairness de alto rendimiento si todos los nodos tienen el mismo rendimiento bajo condiciones similares de tráfico de fuente y carga de la red. Las redes Mesh muestran un alto rendimiento desigual entre los contendientes de flujo de tráfico especialmente cuando los protocolos MAC como el basado en CSMA/CA se utilizan para la contención de resolución.

Existen tres propiedades importantes que son asociadas con los protocolos MAC como el basado en CSMA/CA, cuando se utiliza en un entorno Mesh:

1. La asimetría de la información,
2. Contención de la dependencia de la localización, y
3. Carácter half-duplex de los sistemas de un solo canal.

La asimetría de la información es causada por la falta de información en ciertos nodos, pero también se produce por tener exceso de información lo que causa una falta de Fairness. Por ejemplo, cuando un nodo está expuesto a dos flujos de tráfico, se establece el vector de asignación de red (NAV) y, por tanto, se abstiene de transmitir.

Además, la propiedad de half-duplex de un sistema de una sola interface también causa un alto rendimiento inequitativo en un radio single-radio. Debido a las características half-duplex, ningún nodo puede transmitir y recibir simultáneamente por la red.

2.11.4 FIABILIDAD Y ROBUSTEZ

Las redes inalámbricas Mesh mejoran la fiabilidad y la robustez de la comunicación. La topología de una malla parcial en una red Mesh proporciona alta fiabilidad y diversidad de rutas contra nodos y fallas en los enlaces. Los múltiples radios de una red Mesh ofrecen una importante ventaja de la solidez en la diversidad de la comunicación. Por ejemplo, errores en el canal de un sistema inalámbrico puede ser altamente comparado con redes cableadas, por lo tanto, una degradación de la calidad de la comunicación durante los errores de un canal alto es necesario.

El uso de interfaces de radio múltiple permite la diversidad de frecuencia, por lo que puede causar una pérdida total de la conectividad, debido a la degradación de la señal. Además, los radios pueden usar módulos de conmutación que sean adecuados para lograr la tolerancia a fallos en comunicación, ya sea por cambio de las radios, los canales o mediante el uso de múltiples radios simultáneamente.

2.11.5 ROAMING

El término Roaming corresponde al concepto de Itinerancia, es un concepto utilizado en las comunicaciones inalámbricas para describir la capacidad que tiene un dispositivo o móvil para movilizarse de una zona de cobertura a otra. Cuando el Roaming está activado, es fluido entre los diferentes puntos de acceso manteniendo la conexión si el usuario está en movimiento.

La red inalámbrica consiste de microceldas o áreas de cobertura para que el usuario pueda moverse libremente en un Campus, tanto en el interior como en el exterior de los edificios. Para que sea factible el Roaming y se evite corte de comunicación, debe existir una pequeña zona de superposición conocida como Overlapping que esté cubierta de al menos dos puntos de acceso o Access Points, tal como se muestra en la siguiente figura:

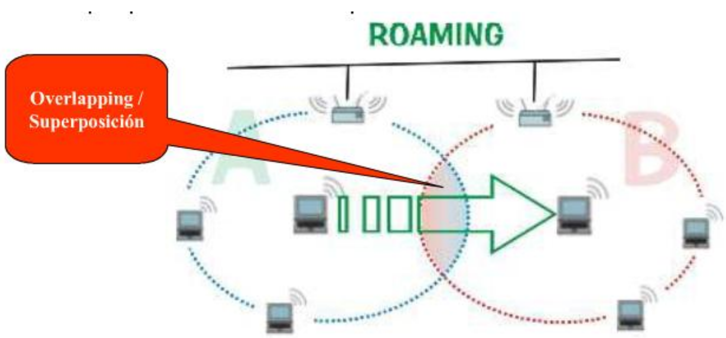


Figura 2-24 Overlapping en una red inalámbrica

Roaming es el proceso por el que un usuario cambia entre los puntos de acceso en una red inalámbrica Mesh. En una gran red Mesh inalámbrica capaz de manejar VoIP, una solución de

Roaming debe ser escalable, fiable, rápido y proporcionar handoff entre las diferentes zonas de cobertura que ofrecen los routers inalámbricos. Esa solución debe ser escalable para varios puntos de acceso de la red. La clave de la escalabilidad es minorizar un Roaming general, reduciendo la carga sobre el sistema en cada handoff. La red inalámbrica también debería ser resistente a fallos de las células de una manera similar a Internet. Esto requiere la capacidad de la red para sacar el máximo provecho de la conectividad en toda la malla. En la actualidad, la latencia debe ser inferior a 50 ms para ser indetectables para los usuarios de VoIP.

Soluciones de Roaming en las redes móviles celulares no se pueden aplicar porque requieren topologías de árboles jerárquicos. Una propuesta conocida como "micro-movilidad" es generalmente diseñada para un uso estrictamente de una red jerárquica donde se introduce los cuellos de botella debido a la falta del balanceo de carga y es vulnerable a la falla o caída de los puntos de acceso, entre otros problemas. La principal debilidad de las redes jerárquicas, sin embargo, es la falta de escalabilidad ya que requieren un estado de caché para el almacenamiento del intercambio de información debido a la duplicación de los puntos de acceso en el sistema. La cantidad de información intercambiada y almacenada crece exponencialmente con el tamaño de la red y con la cantidad de actividades de Roaming entre los usuarios.

Otra solución importante en redes IP, que incluso es una norma IEEE, se llama Mobile IP, la cual es escalable, pero puede sufrir de una larga latencia debido al handoff al momento de envíar datos a un usuario móvil. Técnicas de optimización para reducir la latencia handoff requieren cambios en el software del usuario, que podría ser un grave impedimento para un normal desempeño de la red.

Las redes inalámbricas Mesh habilitan a los usuarios para poder conmutar entre los routers Mesh debido a su movilidad. Cuando el dispositivo de un usuario detecta una señal más fuerte que se encuentra disponible, un proceso de Roaming permite que el dispositivo pueda cambiar a la señal más fuerte. En el momento del Roaming, el dispositivo debe ponerse en contacto con un punto de acceso, que suele ser un servidor situado en algún lugar de la red que contiene el perfil del usuario móvil. Para ponerse en contacto con el punto de acceso el dispositivo del usuario puede recorrer largas rutas a través de los puntos de acceso de la red. Además, cada vez que el usuario aplica el Roaming, el punto de acceso debe estar activado ya que esto introduce grandes retrasos y la degradación de la señal de los usuarios finales.

Handoff es un método para un Roaming distribuido en una red inalámbrica Mesh donde un punto de acceso estudia el perfil de un usuario al momento de realizar un Roaming para poder enviar la información a los demás puntos de acceso y poder predecir el siguiente Roaming del usuario dentro de la red al desear ingresar en una nueva celda, y por tanto liberar la información al punto de acceso que se encontraba conectado. Cada nodo en la red se maneja con interfaces de capa 2 (capa MAC y Enlace), y la capa 3 (capa IP). La red en malla inalámbrica utiliza la interface de roaming de capa 2 que sirve como el encargado para eventos de movilidad sin la intervención de software de cliente. Además incrementa la capacidad de realizar cada vez más funciones, como autenticación, el cambio a nuevos canales de radio, y las actualizaciones de enrutamiento permiten que el handoff sea lo más rápido posible.

CAPITULO 3

3. ESTUDIO Y DISEÑO DE LA TOPOLOGÍA DE LA RED MESH

3.1 CARACTERÍSTICAS DEL LUGAR DE ESTUDIO

La Facultad de Ingeniería Eléctrica y Computación (FIEC) de la ESPOL, se encuentra ubicado en el campus Gustavo Galindo al noroeste de la ciudad de Guayaquil en el centro del Bosque Protector Prosperina en el Km. 30½ de la vía Perimetral de la ciudad. Las coordenadas geográficas del campus son: 2°09'38''S 79°57'01''O.

El área aproximada de la FIEC es de 90000m^2, tiene cerca de 2450 estudiantes y 120 profesores, de los cuales un promedio de 50 usuarios utilizan la red por hora, en la Figura 3-1 se muestra una vista aérea del área de la FIEC.

Figura 3-1 Facultad de Ingeniería Eléctrica y Computación

Dentro de la FIEC se encuentran varios lugares de distracción y estudio entre ellos tenemos:

- 24 aulas de clase
- 1 Comedor
- 17 laboratorios de computación
- 1 Edificio inteligente
- 2 Parqueaderos
- 4 Sectores de distracción
- 2 Salas de estudio

3.2 ANALISIS DE PROVEEDORES

Como se ha resaltado en los primeros capítulos las redes malladas están en pleno desarrollo, se están creando protocolos y estándares que mejoren el funcionamiento de dichas redes, pero en la actualidad los fabricantes de equipos para soluciones de comunicaciones inalámbricas han escogido al estándar de la IEEE 802.11 como norma base para sus equipos, ya que se considera que la mayoría de los equipos terminales a los cuales se le va a ofrecer el servicio de la red mallada soportan dicho estándar.

Empresas fabricantes de equipos de telecomunicaciones como Tropos Networks, Belair Networks, SkyPilot, Strix Systems, ROAMad, Cisco Systems, Nortel Networks, Motorola, entre otras, están desarrollando y mejorando soluciones de redes malladas para liderar el mercado, creando una competencia reñida entre proveedores y beneficiando con esto a los usuarios.

En la siguiente figura se muestra el posicionamiento de los fabricantes más influyentes en el mercado de redes malladas de acuerdo a la penetración que tienen sus equipos mesh.

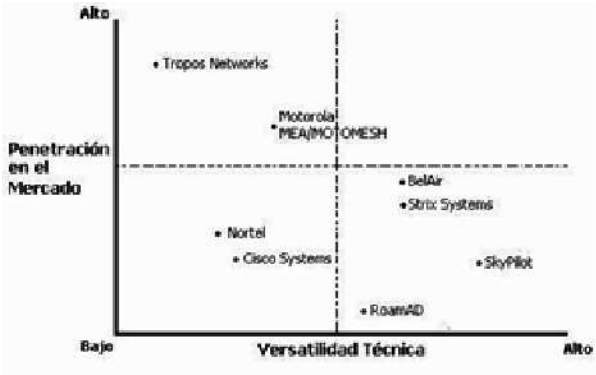


Figura 3-2 Posicionamiento de fabricantes.

Aunque Tropos Networks está liderando en la penetración de sus productos mesh en el mercado seguido por Motorola , BealAir y Strix Systems, Nortel y Cisco Systems están trabajando fuerte en el mejoramiento de sus productos para empezar a liderar el mercado como lo están haciendo en soluciones cableadas y tecnologías como Wimax y WiFi.

3.2.1 TROPOS NETWORKS

Figura 3-3 Logo Tropos Networks.

La solución que ofrece Tropos Networks se denomina “TROPOS METROMESH”, los equipos y protocolos que utiliza proporcionan la capacidad de reaccionar a las fallas que se pueden dar por factores tales como interferencia o pérdida de un acoplamiento.

Para obtener el máximo rendimiento de la tecnología Tropos MetroMesh, el fabricante implemento a sus equipos su propio protocolo de enrutamiento llamado Predictive Wireless Routing Protocol (PWRP), el cual es una variante del protocolo tradicional de las redes cableadas OSPF (Open Shortest Path First).

La arquitectura de la MetroMesh de Tropos se la puede dividir en tres partes, como se muestra en la Figura 3-4.

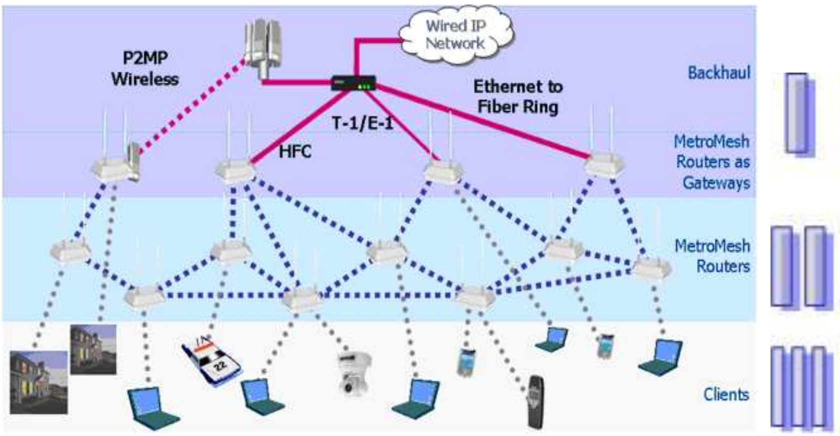


Figura 3-4 Arquitectura de una MetroMesh.

I. Interconexión inalámbrica o cableada entre los Gateway Mesh Routers y la estación base que se conectará a la nube IP.

II. Proporciona múltiples caminos entre los routers para encontrar la mejor ruta y transmitir la información.

III. Interconexión entre los usuarios y la red mallada vía WiFi (IEEE 802.11).

CARACTERISTICAS GENERALES DE LA METROMESH DE TROPOS

De la radio:

- Los equipos de Tropos pertenecen a sistemas de primera y segunda generación, ya que tienen una o dos interfaces de radio. Cuando tiene una sola interfaz de radio, la cual opera en la banda de 2,4 GHz, la emplea para la comunicación entre routers y para proporcionar servicio. Cuando tienen dos interfaces de radio, 2,4 GHz y 5 GHz, las conmuta dinámicamente para la comunicación entre routers o para dar servicio.
- Los equipos terminales (equipos de los usuarios) deben de soportar el estándar 802.11b/g de la IEEE.
- La distancia entre el router mesh y el usuario es máximo de 7 metros para tener un buen servicio.

De configuración:

- La red se configura automáticamente. Cuando selecciona el camino óptimo trata de maximizar el throughput y minimizar la latencia. Dicha ruta la actualiza cada 250 ms y lo hace dinámicamente.
- Para lograr el máximo throughput se toma en cuenta medidas realizadas en el uplink y en el downlink.
- Cuando se presenta un fallo de un enlace el router busca el enlace alternativo óptimo.
- Permite un máximo de 3-4 saltos. No obstante detalla que el overhead introducido es mínimo y constante (no aumenta en cada salto y consume únicamente el 5% del ancho de banda disponible), admite un máximo de 20 nodos/km2.

De seguridad y calidad de servicio:

- Para la seguridad la MetroMesh Tropos utiliza el protocolo AES entre los MetroMesh Routers y WPA para el acceso IEEE 802.11.

- Con respecto a la calidad de servicio permite que el usuario defina diferentes niveles de prioridad para el tráfico.

EQUIPOS Y SOFTWARE QUE UTILIZA LA METROMESH

Tropos Outdoor MetroMesh Routers: optimizado para exteriores

Figura 3-5 Tropos 5320 Outdoor MetroMesh Router

Figura 3-6 Tropos 9532 Outdoor Public Safety MetroMesh Router

Figura 3-7 Tropos 5210 Outdoor MetroMesh Router

Tropos Indoor MetroMesh Routers: optimizado para interiores

Figura 3-8 Tropos 3210 Indoor MetroMesh Router

Tropos Mobile MetroMesh Routers: para movilidad de los meshRouters

Figura 3-9 Tropos 4210 Mobile MetroMesh Router

Figura 3-10 Tropos 9422 Mobile Public Safety MetroMesh Router

Software

- Las herramientas del análisis y del control de Tropos MetroMesh (Tropos Control Network Management System y Tropos Drive Network Testing Tool), fueron diseñadas para dar a los encargados de la red, una centralización y visibilidad en todos los aspectos del funcionamiento de esta. Además permite el análisis, la optimización y el control de los sistemas altamente dispersados del acoplamiento.

3.2.2 BELAIR NETWORKS

Figura 3-11 Logo BelAir Networks

BelAir Networks define una red mallada 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 malladas son:

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

Además considera que una red mallada 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.

La solución de red mallada que ofrece BelAir es interesante ya que utiliza equipos que tienen desde uno hasta cuatro radios para conectarse entre ellos y para proporcionar servicio, en la siguiente figura se muestra la arquitectura de la red utilizando uno de sus equipos con mayor tecnología el BelAir 200.

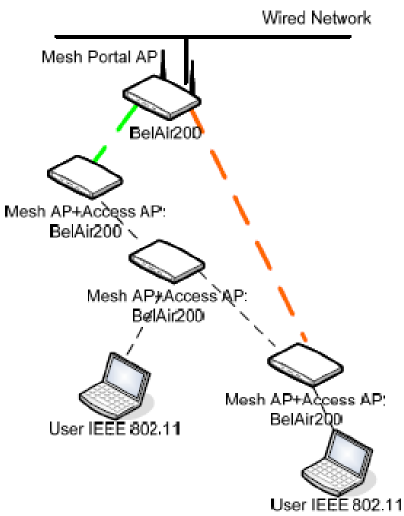


Figura 3-12 Arquitectura de una red mallada de BelAir.

<u>CARACTERISTICAS GENERALES DE LA RED MALLADA DE BELAIR</u>

De la radio:

- Básicamente es una solución multi-radio, cada nodo consta de dos o más radios.

- Los equipos terminales (equipos de los usuarios) deben de soportar el estándar 802.11b/g de la IEEE.
- Es una solución diseñada para outdoor, pero que permite que la señal penetre en el interior de los edificios para dar cobertura también en indoor.

De configuración, seguridad y calidad de servicio:

- Permite un máximo de 5 saltos.
- Se considera que es una solución de nivel 2, es decir, de la capa de enlace de datos.
- Con respecto a la seguridad aplica autenticación 802.1x/EAP/PEAP/WPA y encriptación 802.11i/WPA2/AES-152/WEP.
- Tiene la capacidad de soportar VLANs, múltiples SSIDs y VPNs.
- Con respecto a la calidad de Servicio, permite definir clases de servicio, prioridades y VLANs para diferentes tipos de tráfico.

<u>EQUIPOS QUE UTILIZA LA RED MALLADA DE BELAIR</u>

Figura 3-13 Bel Air 200-13

Figura 3-14 Bel Air 100T-21

Figura 3-15 BA 100

3.2.3 SKYPILOT

Figura 3-16 Logo SkyPilot Networks

Skypilot es considerado un proveedor de banda ancha inalámbrica carrier-class. Ofrece una variedad de productos y soluciones que permiten desplegar de manera rápida y eficiente una red por la que el usuario podrá utilizar servicios de VoIP, videovigilancia y servicio WiFi público.

En la solución mesh que ofrece Skypilot denominada SyncMesh, se utiliza el protocolo TDD (Time Division Duplex) el cual es el encargado de sincronizar todas las transmisiones para maximizar el rendimiento.

Además SyncMesh permite la sincronización de los relojes de los diferentes equipos mediante GPS (Sistema de Localización Global), de manera que se pueden manejar múltiples conversaciones en el mismo instante de tiempo y en la misma frecuencia.

Una caracteriza especial de la solución mesh es que se pueden utilizar en sus nodos un arreglo de 8 antenas para conseguir mejores zonas de cobertura y capacidades superiores a sus competidores. Cabe recalcar que cada equipo cumple con la función de router mesh y AP al mismo tiempo. La solución de SkyPilot presenta la siguiente arquitectura de red:

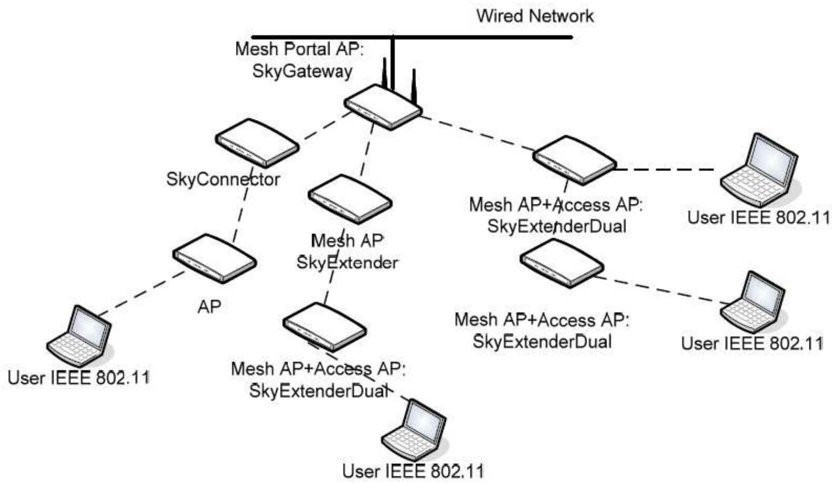


Figura 3-17 Arquitectura de una red mallada de SkyPilot.

CARACTERISTICAS GENERALES DE LA RED MALLADA DE SKYPILOT

De la radio:

Los equipos de SkyPilot constan de una antena sectorizada (8 antenas a 45°) que permite la reutilización del ancho de banda.

Emplea la banda de 5.4 GHz para el backbone mesh y la banda de 2.4 GHz para el servicio al usuario.

Permite utilizar niveles de potencias altos para hacer frente a las atenuaciones introducidas por los obstáculos.

Los equipos terminales (equipos de los usuarios) deben de soportar el estándar 802.11b/g de la IEEE.

Es una solución desarrollada para entornos indoor y outdoor.

De configuración:

La solución mesh de SkyPilot es una red dinámica en la que los enlaces se configuran de manera automática. Si se desea incorporar nuevos nodos en la red, los caminos y las rutas se actualizan automáticamente, no siendo necesaria la reconfiguración manual de los equipos.

En cada instante cada nodo sólo puede tener un enlace activo con otro. Por este enlace le llegan los paquetes a partir de los cuales analiza cómo está el resto de la red.

Cada nodo mesh está continuamente pasando un test de conectividad a los enlaces, analiza la eficiencia de todas las posibles rutas alternativas, con la finalidad de actualizar y optimizar las tablas de enrutamiento tomando como medidas principales la capacidad y el Throughput.

Mediante este sistema la red es capaz de recuperarse dinámicamente frente a los fallos en la red a la vez que es capaz de realizar un balanceo de la carga para no sobrecargar los enlaces.

La arquitectura de la red permite un número máximo de 11 nodos/km2. Además se admite un número máximo de 4-5 saltos entre nodos.

De seguridad y calidad de servicio:

Con respecto a la seguridad aplica el protocolo AES y certificados para la autenticación.

Para ofrecer calidad y servicio permite que algunos clientes puedan estar conectados directamente al backbone mesh. La QoS entre el usuario y el nodo mesh depende del acceso Wi-Fi empleado.

EQUIPOS Y SOFTWARE QUE UTILIZA LA RED MALLADA DE SKYPILOT

Figura 3-18 SkyGateway

Figura 3-19 SkyGateway Dualband

Figura 3-20 SkyExtender

Figura 3-21 SkyExtender DualBand

Figura 3-22 SkyAccess DualBand

Figura 3-23 SkyConnector Classic

SkyProvision y SkyControl

SkyProvision: software de provisión para dar acceso a los clientes, a los que permite obtener su información de configuración de los servidores correspondientes.

SkyControl: software de monitorización y gestión de la red mesh (software en función del número de licencias), ofreciendo estadísticas y valores de latencias, throughputs, entre otros. Basado en SNMP.

3.2.4 STRIX SYSTEMS

Figura 3-24 Logo Strix Systems

Strix Systems ha desarrollado una solución mesh con equipos que manejan dos interfaces de radio, dicha solución es denominada Acces/One Network OWS.

Con la topología Mesh Strix Systems busca que la red sea inherentemente fiable y redundante, además, que se pueda extender para conectarle miles de dispositivos. La red Access/One que ha desarrollado esta empresa se puede instalar en horas y no necesita que se elaboren planificaciones ni mapas de la localización con el fin de asegurar comunicaciones fiables.

En la siguiente figura se muestra la arquitectura de la red mallada de Strix Systems.

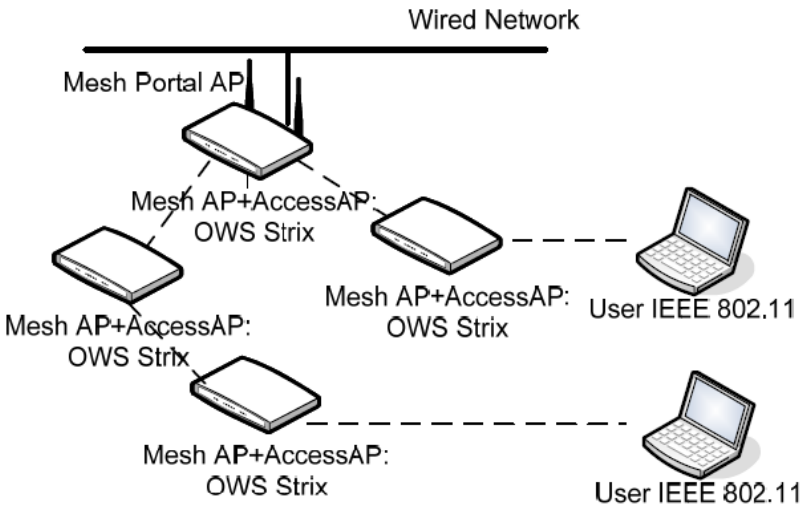


Figura 3-25 Arquitectura de una red mallada de Strix Systems.

CARACTERISTICAS GENERALES DE LA RED MALLADA DE STRIX SYSTEMS

De la radio:

- Cumplen con dos funciones, router mesh y Access Point.
- Tienen 2 interfaces de radio, en la banda de 2,4 GHz y en la banda de 5 GHz.

- En la interfaz de radio que se usa para interconectar nodos utiliza múltiples canales de radio y los divide para realizar la transmisión o recepción de datos.
- Se puede sectorizar las antenas para optimizar la cobertura.
- La distancia entre nodos puede ser hasta 50 metros.
- Los equipos terminales (equipos de los usuarios) deben de soportar el estándar 802.11 a/b/g de la IEEE.
- Existen radios para entornos indoor y outdoor.

De configuración:

- La solución mesh de Strix Systems permite tener una red escalable y autoconfigurable.
- Los parámetros que se consideran para obtener el camino óptimo para realizar una trasmisión son: el throughput, la relación señal a ruido y la disponibilidad de los enlaces.
- Proporciona regeneración automática frente a fallos. En caso de que exista pérdida de comunicación entre dos nodos, selecciona la ruta alternativa más adecuada.

- Permite un máximo de 50-150 usuarios por cada nodo. Permite un máximo de 10 saltos, lo que produce latencias de unos 20 ms.

De seguridad, calidad de servicio y movilidad:

- Con respecto a la seguridad de la red Strix Systems emplea un servidor independiente para gestionar la autenticación. Para la encriptación emplea IEEE 802.11i (WPA2) con AES-152 bits y WEP.

- Con respecto a la Calidad de Servicio proporciona diferentes niveles de prioridad para los diferentes tipos de tráfico (definidos por el usuario).

- Con respecto a la movilidad, los Access AP pueden moverse aproximadamente a 300 km/h, lo que hace que sean adecuados para su ubicación en vehículos.

EQUIPOS QUE UTILIZA LA RED MALLADA DE STRIX SYSTEMS

Figura 3-26 Strix EWS-150

Figura 3-27 Strix EWS-100

Figura 3-28 Strix MWS-100

Figura 3-29 OWS-2400

Figura 3-30 OWS-3600

3.2.5 CISCO SYSTEMS

Figura 3-31 Logo 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.

EQUIPOS QUE UTILIZA LA RED MALLADA DE CISCO SYSTEMS

Cisco Aironet 1300 Outdoor Access Point/Bridge

Es un punto de acceso y bridge basado en el estándar IEEE 802.11g, que provee conectividad inalámbrica eficiente y económica de alta velocidad entre redes o clientes múltiples, ya sean fijos o móviles. Los Cisco Aironet 1300 Series como se mencionó, soportan el estándar 802.11g que provee velocidades de transmisión de datos de hasta 54 Mbps, al tiempo que mantiene compatibilidad hacia atrás con los dispositivos 802.11b. Basado en el software Cisco IOS, el

Cisco Aironet 1300 Series brinda funcionalidades avanzadas como Fast Secure Roaming (roaming rápido y seguro), QoS (calidad de servicio), y LANs virtuales (VLANs). La flexibilidad de los Cisco Aironet 1300 les permite operar como bridge inalámbrico, access point, o bridge grupal.

Figura 3-32 Cisco Aironet 1300 Outdoor Access Point/Bridge

Cisco Aironet 1400 Wireless Bridge

La serie 1400 provee de un alto funcionamiento y de soluciones efectivas para conexión de múltiples LANs en un área metropolitana. Construyendo una infraestructura Wireless en un área metropolitana con Cisco Aironet 1400 permite a los usuarios disponer de una solución fácil de implementar y que cumple con los requisitos de seguridad de área amplia que los profesionales de networking requieren, bajo los estándares 802.11 y 802.11i. Es un equipo diseña para ambientes exteriores.

Figura 3-33 Cisco Aironet 1400 Wireless Bridge

Cisco Aironet 1500 Series lightweight outdoor mesh access point

El Cisco Aironet 1500 proporciona la seguridad, la posibilidad de gestión, la fiabilidad y la facilidad de despliegue para crear WLANs de alto rendimiento para redes exteriores inalámbricas.

El Cisco Aironet 1500 Serie opera bajo los Cisco WLAN Controllers y el Cisco Wireless Control System (WCS) Software, centralizando las funciones claves de las redes WLANs para proporcionar la dirección escalable, la seguridad, y la movilidad inalámbrica entre despliegues de interiores y exteriores. Diseñado para realizar la configuración a través de interfaces de línea de mando (CLIs) o WCS gráfico.

Emplea la seguridad para Wifi con el protocolo WPA2 y el empleo del Estándar de Cifrado basado por hardware Avanzado (AES).

3.2.6 MOTOROLA

Figura 3-34 Logo 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, MOTOMESH brinda datos en tiempo real a los socorristas, residentes, empleados y clientes, y posibilita aplicaciones vitales de banda ancha inalámbrica.

En la siguiente figura se muestra la arquitectura de la red mallada de Motorola.

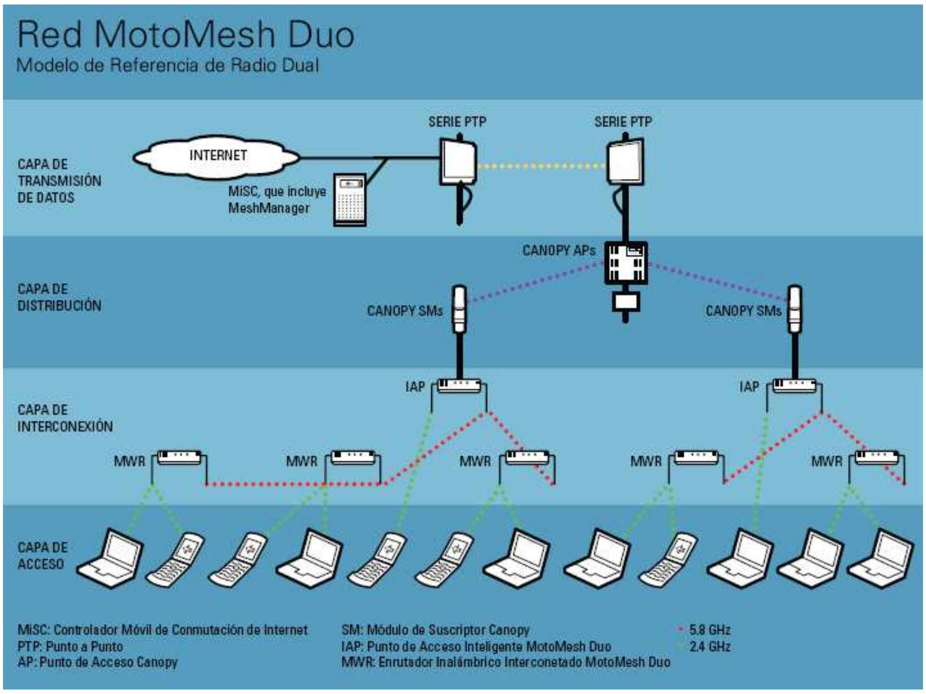


Figura 3-35 Arquitectura de una red mallada de Motorola.

CARACTERISTICAS GENERALES DE LA RED MALLADA DE MOTOROLA

- Motorola ofrece soluciones para trabajar en las bandas 2.4/5.4 GHz, 2.4/4.9 GHz y 2.4/5.8 GHz.

- ***Gateways de Internet flexibles y adaptables***, los nodos gateway se adaptan a las potenciales pérdidas de la conexión backhaul para transmisión de datos al convertirse instantáneamente en enrutadores inalámbricos (routers) y dirigir el tráfico a otra gateway en la red. Ello minimiza las interrupciones del servicio y garantiza conectividad WiFi continua.

- ***Herramientas de administración avanzadas***, Motorola tiene una herramienta de configuración online que proporciona acceso en cualquier momento y lugar a los parámetros de configuración de un dispositivo mesh*.* Dicha herramienta también posibilita la administración remota de sistemas pequeños.

EQUIPOS QUE UTILIZA LA RED MALLADA DE MOTOROLA

Figura 3-36 MOTOMESH™ Duo 4.9 GHz

Figura 3-37 MOTOMESH™ Duo 5.4 GHz

Figura 3-38 MOTOMESH™ Duo 5.8 GHz

Figura 3-39 IAP4300

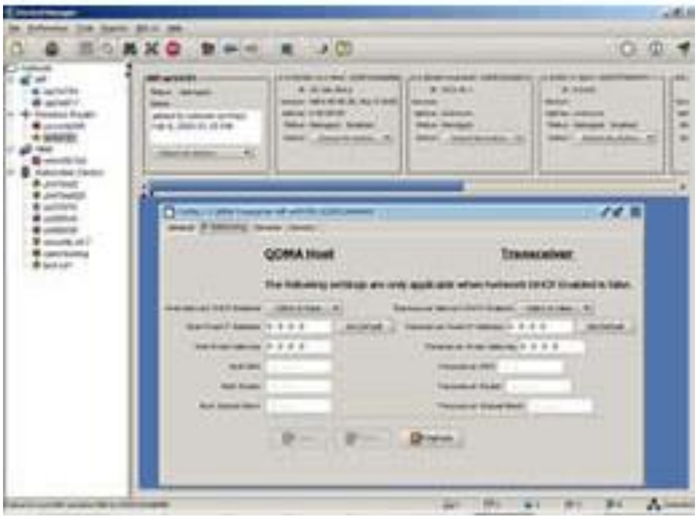


Figura 3-40 MeshManager

3.2.7 NORTEL

Figura 3-41 Logo NORTEL

La tecnología Mesh de NORTEL permite entregar a los clientes una solución empresarial completa que ofrece una segregación de tráfico segura y permite que distintos departamentos utilicen la misma red sin límites de movilidad.

Wireless Mesh permite un roaming transparente entre los puntos de acceso, lo que significa que los usuarios no pierden conexiones inalámbricas a medida que se mueven de un punto de acceso a otro. Asimismo, la solución Nortel Wireless Mesh utiliza el estándar Wi-Fi 802.11b, lo que permite a los usuarios que tienen computadores portátiles o dispositivos de mano habilitados con Wi-Fi, tener acceso a la red sin necesidad de contar con hardware o software nuevo.

En la siguiente figura se muestra la arquitectura de la red mallada de NORTEL.

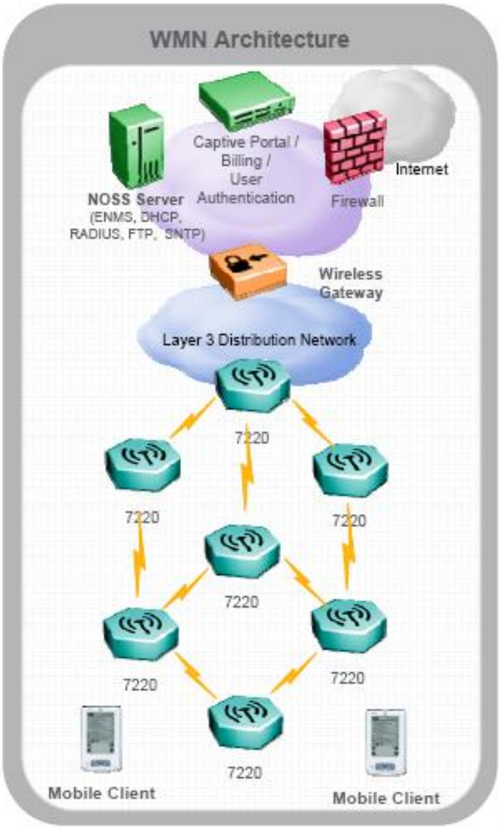


Figura 3-42 Arquitectura de una red mallada de NORTEL.

APLICACIONES DE LAS WMN DE NORTEL

La solución WMN de Nortel tiene muchas aplicaciones en el mundo exigente de las telecomunicaciones entre ellas tenemos:

- Espacios abiertos como parques o plazas públicas.
- Centros comerciales.
- Campus universitarios o lugares de investigación.

- Aeropuertos, estaciones de bus, estaciones de tren.
- Paradas de camiones, grandes bodegas, paraderos.
- Estadios u otros lugares recreacionales.
- Áreas metropolitanas.

EQUIPOS QUE UTILIZA LA RED MALLADA DE NORTEL

Figura 3-43 Access Point 7220

Figura 3-44 Access Point 7215

Figura 3-45 Wireless Gateway 7250

3.2.8 TABLA COMPARATIVA DE PROVEEDORES

A continuación se muestra una tabla comparativa de los proveedores que hemos mencionado anteriormente entre los parámetros que se detallan tenemos:

Fabricante: *Nombre de las principales empresas proveedoras de solución mesh.*

Solución: *Nombre comercial de la solución mesh.*

Tipo de antena: *Indoor, Outdoor o ambas.*

Configuración automática: *Muestra si la solución propuesta tiene la capacidad de ser autoconfigurada cuando se presente algún inconveniente.*

N° máximo de nodos: *Cantidad de nodos o antenas que se pueden colocar por* Km^2 *o por determinado equipo.*

N° máximo de saltos: *Cantidad de saltos que puede dar un paquete para ser entregado a su destino dentro de la solución mesh.*

Equipos utilizados: *Equipos principales que se utilizan al momento de implementar la red.*

3.2.9 ELECCIÓN DEL PROVEEDOR PARA EL DESARROLLO DE LA RED MESH

En las Tablas VII y VIII se muestra los principales proveedores de soluciones mesh, además, se nota que tienen una característica en común, la mayoría utiliza dos interfaces de radio, una para interconectar los nodos y otra para los usuarios (2.4 GHz y 5 GHz respectivamente). Los proveedores mencionados tienen similares características con sus excepciones por ejemplo, la mayoría acepta saltos entre 3 y 5 pero Strix Systems el máximo de saltos es de 10.

Para el desarrollo del diseño de la red mesh en la Facultad de Ingeniería Eléctrica y Computación de la ESPOL se eligió como proveedor a NORTEL por ser el único proveedor interesado, por medio de partners, en introducir al mercado ecuatoriano la solución mesh. Además por poseer una solución que una vez implementada con el tiempo se puede ir extendiendo sin ningún inconveniente.

3.3 CARACTERÍSTICAS GENERALES DE LAS REDES MESH DE NORTEL

Como características generales de las redes mesh de Nortel podemos citar:

- ***Auto-configurable y auto-regenerable*** gracias al uso de antenas inteligentes.
- Los nodos que se utiliza para la implementación de la red son de ***fácil instalación***.
- La infraestructura y la tecnología aplicada permite la ***movilidad del usuario*.**
- La red cumple con ser ***redundante*.**
- Utiliza el ***estándar 802.11*,** puesto que es el estándar utilizado por la mayoría de dispositivos terminales.
- ***Alta seguridad*** con autenticación y encriptación.

3.4 ELEMENTOS DE LAS REDES WIRELESS MESH

La red inalámbrica Wireless Mesh consta de los siguientes elementos que se detallarán a continuación:

3.4.1 SERVIDOR NOSS

El servidor NOSS (Network Operations Support System) es un sistema de soporte que proporciona servicios centralizados de monitoreo, control y gestión de operaciones de red, con ayuda de protocolos específicos logra la comunicación con los elementos desplegados en la red inalámbrica Mesh.

El sistema NOSS es un servicio propio de los equipos de tecnología Mesh red Nortel, el cual consiste de los servidores que se detallan a continuación:

Tabla IX: Servidores que proporciona el Servidor NOSS

Elemento	Requerimiento	Descripción
Servidor DHCP	Soporte RFC3011	Proporciona direcciones IP dinámicas para asignarlas a los puntos de acceso y nodos móbiles.
Servidor Radius	Protocolos de Seguridad EAP	Proporciona la autenticación, autorización y asignación de cuenta a los usuarios móbiles.
Servidor FTP	No presenta	Almacena los archivos de configuración cuando se realiza un upgrade de los equipos.

3.4.1.1 SERVIDOR RADIUS

El servidor RADIUS se desempeña como un servidor AAA (Authentication, Authorization and Accounting), es decir que se encarga de la autenticación, autorización y asignación de cuentas de todos los usuarios de la red Mesh

El servidor Radius deberá ser el encargado de proporcionar:

- El soporte para el protocolo EAP que emplea los protocolos EAP-TTLS y EAP-PEAP en los nodos móviles y el protocolo EAP-LEAP en los puntos de acceso.

- Las contraseñas de las diferentes sesiones otorgadas a los usuarios para que tengan el acceso a la red en función del mecanismo de autenticación que se esté aplicando.

Cabe mencionar que con el fin de completar la autenticación de un nodo móvil, el dispositivo del usuario debe corresponder a un perfil almacenado en el servidor de autenticación. Luego de que el usuario es autenticado, un identificativo en el túnel-ID es almacenado en el perfil y se devuelve al punto de acceso AP.

3.4.1.2 SERVIDOR DHCP

El servidor DHCP (siglas en inglés de Dynamic Host Configuration Protocol) emplea un protocolo de red que permite a los nodos y usuarios de la red Mesh obtener sus parámetros de configuración IP automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

El servidor DHCP debe:

- Brindar soporte a la norma RFC 3011 para apoyar a resolver la opción de subnetting de la red.
- Tener un temporizador para dar cabida a los retrasos ocasionados por múltiples saltos de los puntos de acceso.

Para la configuración de un punto de acceso AP a través del servidor DHCP debe poseer lo siguiente:

- Dirección del pool mediante subnetting.
- Máscara de subred.
- Routers por defecto.
- Tiempo por asignación de la dirección IP.
- Ubicación del archivo de configuración por FTP.
- Identificar el área OSPF.

- Dirección IP del Wireless Gateway 7250.

Adicional para la configuración de los nodos móviles se toma en cuenta lo siguiente:

- El pool de direcciones IP con su respectiva máscara de red asignada para una red que posee un SSID.
- Dirección IP del Wireless Gateway 7250.
- Tiempo por asignación de la dirección IP.

3.4.1.3 SERVIDOR FTP

Un servidor FTP (File Transfer Protocol) tiene como función principal el mover uno o más archivos con seguridad entre distintos equipos terminales proporcionando organización de los archivos y control de la transferencia.

El servidor FTP permite la descarga de las diferentes versiones de software de todos los elementos de la red Mesh, ya sea de configuración o actualización, para lo cual se encarga de realizar lo siguiente:

- Descargar el archivo de configuración para un AP (El servidor FTP alberga el archivo de configuración que se utiliza para configurar dinámicamente un punto de acceso AP cuando se inicializa.)

- Actualizar software de un AP (El servidor FTP acoge el software para cargar la imagen de un punto de acceso AP).
- Realizar un Upgrade del software, realizar copias de seguridad o restablecer las operaciones del equipo Wireless Gateway.

Los siguientes parámetros se deben configurar en el servidor FTP así como en el punto de acceso AP:

- Ubicación del servidor FTP (dirección IP).
- Nombre del usuario para el acceso al archivo y a la imagen del equipo.
- Contraseña para acceder al archivo de configuración o al software de la imagen.

3.4.2 PUERTA DE ENLACE WIRELESS GATEWAY 7250

La puerta de enlace es encargada de conectar la red Mesh con la red del proveedor del servicio de Internet. Además es responsable del enrutamiento, la seguridad del enlace de tránsito, el estado del firewall, la seguridad de los datos hacia el usuario y la movilidad de los usuarios inalámbricos.

Los dispositivos 7250 anuncian la accesibilidad inalámbrica para una o más subredes IP asignadas para los usuarios y entidades de la red Mesh, es decir que se encarga de la seguridad y movilidad.

En lo que respecta al hardware del equipo tiene interfaces de Ethernet 10/100 con ranuras de expansión y soporta alrededor de 90 puntos de acceso como máximo.

A continuación se presenta el equipo Gateway 7250:

Figura 3-46 Wireless Gateway 7250

3.4.3 NAP-ROUTER

El router NAP-R incorpora funciones de enrutamiento y varias interfaces Ethernet que permiten la conexión de varios puntos AP@NAP. Este equipo trabaja como un router IP que soporta el protocolo de enrutamiento OSPF.

El equipo se encarga de la configuración de las rutas por defecto y rutas internas de los puntos de acceso con el objetivo de prevenir que puntos de acceso externos se filtren dentro la red y evitar el aumento de las tablas de enrutamiento y los requerimientos por uso de memoria. Este tipo de enrutamiento dinámico es útil para redes con un número limitado de puntos de salida.

Para el transporte de tráfico IP entre el Wireless Gateway y los enrutadores NAP-R puede utilizarse enrutamiento en capa 3, o a través del Nivel 1 o 2 donde se utilizan enlaces punto a punto virtuales.

En lo que respecta a las normas de diseño dentro de la red Mesh debe existir un mínimo de dos routers NAP-R, en la cual un equipo se presenta como backup para que sea alternativa en caso que el otro equipo falle. Adicional se recomienda un máximo de 8 a 9 routers NAP-R en la red.

Cabe mencionar que cuando un AP está conectado al router NAP-R se lo conoce como un punto AP@NAP los cuales están conectados a través de un cable Ethernet. Esta conexión a su vez distribuye tráfico a un cluster de puntos de acceso AP 7220 que están debidamente distribuidos en la red.

A continuación se presenta una imagen del router NAP que se utiliza en una red Mesh de Nortel:

Figura 3-47 Router NAP-R

3.4.4 PUNTOS DE ACCESO WIRELESS AP 7220

El AP 7220 permite tener dos tipos de enlaces, el enlace de acceso y el de tránsito. Para el enlace de acceso el cual se lo utiliza para dar servicio a los clientes se emplea el estándar 802.11b/g en el espectro de 2,4 GHz y para el de tránsito que sirve para la comunicación entre los puntos de acceso se utiliza la banda de los 5GHz empleando el estándar 802.11a.

El Punto de Acceso 7220 se puede desempeñar sin problemas en zonas de interiores o exteriores ya sea en ambientes urbanos o rurales, el cual permite un número máximo de 64 usuarios que no utilizan RSNA o 28 usuarios RSNA, aunque el proveedor recomienda un plan de despliegue donde no más de 20 usuarios transmitan simultáneamente a través de un punto de acceso.

En lo que respecta a la funcionalidad los puntos de acceso son encargados del tránsito inalámbrico con su debido enrutamiento en la cual se establecen funciones de seguridad para la validación de las conexiones hacia los otros puntos de acceso AP. Además se establece seguridad de las funciones de control de acceso de los dispositivos de los usuarios.

A continuación se detallan los puntos a tener en cuenta al momento de instalar los AP 7220 y la Tabla X que muestra las características principales del AP con respecto a su enlace de tránsito y enlace de acceso:

La distancia mínima permitida entre los puntos de acceso debe ser de 8 metros, ya que en caso de tener una distancia menor a la recomendada se reduce el rendimiento, debido a problemas de superposición e interferencia.

Cada punto de acceso debe estar a la misma altura de sus puntos vecinos ya que necesitan compartir el enlace de tránsito de manera óptima. La diferencia de altitud entre puntos AP debe ser de ± 5° y no más de ±8°.

Tabla X: Características de los enlaces del punto de acceso AP7220

Ambiente RF Exterior	Rango del Enlace de Acceso (Radio)	Rango del Enlace de Tránsito (AP a AP)	Densidad
Enlace Limpio	300-500 metros	500-800 metros	5 por Km2
Suburbano con LOS	200 metros	300 metros	10 por Km2
Urbano con LOS	300 metros	500 metros	17 por Km2

Para que los AP 7220 tengan un funcionamiento óptimo dentro de la red se tienen las siguientes sugerencias:

- Cualquier AP 7220 debe tener un máximo de tres saltos hasta el punto AP7220@NAP ya que puede reducir el rendimiento del enlace de tránsito. Además puede asociarse con un máximo de 21 APs 7220 aunque un número promedio es de 7 puntos de acceso.

- El uso del protocolo OSPF permite crear un área para el uso promedio de 24 puntos de acceso AP 7220 aunque se permite un máximo de 50 puntos. Cada punto AP 7220 que aplica el protocolo OSPF se comporta como un router de capa 3.

- En una red Mesh un punto AP 7220 @ NAP debe colocarse en el lugar donde haya más tráfico o mayor cantidad de usuarios, con esta consideración en los puntos donde hay mayor demanda el enlace es más eficiente y por tanto se evitan cuellos de botella (bottlenecks) en los equipos.

- La distancia entre un punto de acceso AP 7220 @ NAP y un router NAP no debe ser mayor de 100 metros, en la cual se utiliza un cable 100 Base-TX en modo full dúplex.

A continuación se presenta una imagen del punto de acceso AP 7220:

Figura 3-48 Punto de acceso AP 7220

<u>ENLACES DE TRÁNSITO Y DE ACCESO</u>

El Enlace de Tránsito se utiliza en la red Mesh para interconectar puntos de acceso (APs) e ir formando una red de acceso para proporcionar servicios de datos, video y voz, donde la antena está configurada por seis antenas integradas las cuales apuntan en diferentes direcciones para cubrir un área de 360^o.

El punto de acceso selecciona automáticamente el mejor haz para conectarse con sus vecinos, creando enlaces de tránsito (TL) independientes para conectarse con cada punto de acceso, donde el tiempo de conexión entre los conmutadores es una ranura de tiempo (time slot) la cual es configurable.

La topología de red que se disponga impide que algún punto quede aislado en la red o permita redundancia. La configuración de los puntos de acceso permite que en el enlace de tránsito se cree un spaning tree dinámico que automáticamente bloquea todos los enlaces que no transmiten tráfico.

El Enlace de Acceso es el encargado de conectar al usuario final (dispositivos móviles) al punto de acceso AP inalámbrico. La antena instalada dispone de una cobertura omnidireccional abarcando un rango de cobertura de 360°.

El modo de acceso IEEE 802.11b admite una tasa de transmisión de datos hasta 11 Mbps, en cambio IEEE 802.11g soporta una tasa de transmisión de datos hasta 54 Mbps.

Para el enlace de tránsito (banda de 5Ghz) y para el enlace de acceso (banda de 2.4Ghz) se puede seleccionar el canal de RF en los que operará teniendo en cuenta la gama de frecuencias disponibles para evitar interferencia de RF. La configuración de este parámetro puede ser manual o automática, es preferible hacerlo de manera manual para tener una planificación de todos los equipos inalámbricos de la red.

A continuación se detalla de manera gráfica el enlace de tránsito y el enlace acceso que utiliza un punto de acceso AP para la propagación de la señal hacia los puntos vecinos y hacia los usuarios:

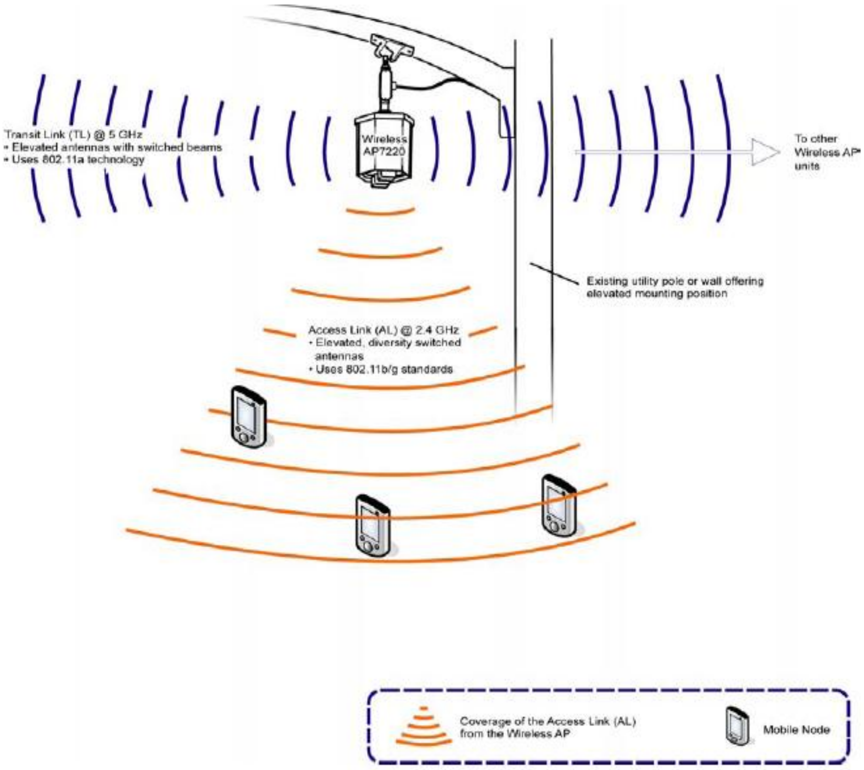


Figura 3-49 Propagación de la señal del Enlace de Tránsito y del Enlace de Acceso

3.5 ESTRATEGIAS DE DISEÑO PARA LAS REDES MESH

Para iniciar con el desarrollo del diseño de la red mesh en la Facultad de Ingeniería Eléctrica y Computación de la ESPOL hay que considerar varios diseños de red enfocados a solucionar problemas o necesidades de cobertura, rendimiento de la red, seguridad, optimización de recursos, entre otros, los cuales se mencionarán a continuación:

3.5.1 DISEÑO ENFOCADO EN LA COBERTURA

Cobertura es el área dentro del cual una red inalámbrica Mesh ofrece servicio. Al momento de planificar el despliegue, se debe considerar la expectativa y la cobertura aceptable de la red (definido por los requisitos del cliente).

3.5.1.1 ENTORNOS DE PROPAGACIÓN RADIO FRECUENCIA

El despliegue de una red inalámbrica Mesh implica los siguientes entornos RF:

ENLACE LIMPIO:

El ambiente de un enlace limpio no presenta obstrucciones en o cerca de la línea de vista (LOS) entre el transmisor y el receptor, es decir entre los puntos de acceso AP 7220. Los puntos de acceso se deben instalar por lo menos a 10 metros sobre el nivel del suelo para lograr un enlace limpio.

LÍNEA DE VISTA URBANA (LOS):

La línea de vista LOS urbana representa la propagación de la señal en ambientes urbanos modernos con edificaciones, como por ejemplo una avenida donde existe una línea de visión entre el transmisor y el receptor. Las obstrucciones cerca de la línea de vista causan pérdida de radio frecuencia RF; además las reflexiones por causa del suelo y las paredes causan disminución de radio frecuencia RF.

SUBURBANO:

El entorno suburbano consiste típicamente de casas y árboles. El ambiente suburbano tiene una relación entre las condiciones de línea de vista LOS y de no línea de vista NLOS para Enlaces de Acceso. En este entorno los puntos de acceso inalámbrico AP 7220 son típicamente instalados en postes de luz estándares o por encima de techos.

INDOOR ABIERTO:

Un entorno interior abierto representa un espacio interior con un techo alto y condiciones de propagación sin obstáculos como por ejemplo aeropuertos, centros comerciales y almacenes. Obstáculos menores debido a la superestructura o divisiones internas se traducen en pérdida mínima de radio frecuencia RF.

INDOOR SATURADO:

Un entorno interior saturado representa un espacio interior con un bajo techo y divisiones interiores como por ejemplo oficinas y viviendas residenciales. La propagación es generalmente sin línea de vista lo que ocasiona una importante pérdida de radio frecuencia RF.

3.5.1.2 EXPECTATIVAS DE SERVICIO DE UN NODO MÓVIL

Los clientes de la red inalámbrica mallada definen el servicio esperado de un nodo móvil. Para el diseño del despliegue de la red mallada se considera lo siguientes puntos con respecto a los nodos móviles.

- Zonas de Cobertura del Enlace de Acceso
- Apoyo a la movilidad del nodo móvil
- Disponibilidad del Enlace de Acceso

3.5.1.2.1 ZONAS DE COBERTURA DEL ENLACE DE ACCESO

El tamaño de la zona de cobertura depende del número de puntos de acceso AP 7220 requeridos para la red y el nivel de servicio ofrecido en el área de cobertura. Hay que señalar que en condiciones ideales el máximo rango del enlace de acceso es 200 metros asegurando una tasa de transmisión máxima de 11Mbps. Al diseñar la cobertura para el enlace de acceso, hay que considerar las siguientes acotaciones, para garantizar un servicio eficiente, las cuales se detallan en el Anexo 6:

Planificación del tamaño de cobertura de enlace de acceso y del nivel de servicio.

Proporcionar la tasa de datos del rendimiento Throughput.

Factores para seleccionar el tipo de antena del enlace de acceso.

3.5.1.2.2 APOYO A LA MOVILIDAD DEL NODO MÓVIL

Un nodo móvil debe mantener una conexión hacia un punto de cobertura, mientras se está movilizando hacia otro sitio, la red desplegada planificará la conexión a zonas de cobertura contiguas y así mantener al usuario conectado todo el tiempo. Basados en los requisitos del usuario final se considera la posibilidad de la aplicación del servicio continuo (para apoyar la movilidad).

3.5.1.2.3 DISPONIBILIDAD DEL ENLACE DE ACCESO

El enlace de acceso debe tener una planificación alternativa, es decir los nodos móviles deben de conmutar hacia otro AP 7220 cuando el punto de acceso con el cual estaban trabajando tiene un fallo.

Sobre los requerimientos del cliente, la posibilidad de tener un punto de acceso backup es fundamental para asegurar la disponibilidad de enlace de acceso.

3.5.1.3 FACTORES QUE AFECTAN EL RANGO DEL ENLACE DE TRÁNSITO

El enlace de tránsito permite la comunicación entre los puntos de acceso, si este enlace tiene problemas con la transmisión del tráfico se puede usar una **antena auxiliar integrada** con mayor potencia para ampliar el alcance del enlace de tránsito o proporcionar una mayor tasa de transmisión de datos a largo del enlace que nos permita lograr una distancia hasta 1000 m con una tasa de transmisión de datos de 36 Mbps con un 50% de disponibilidad.

Este tipo de antenas trabajan con una frecuencia en la banda de los 5GHz, por lo cual factores limitantes de radio frecuencia RF afectan los enlaces de tránsito, entre los cuales tenemos:

<u>LIMITACIONES DE DISTANCIA:</u>

Las seis antenas integradas del enlace de tránsito del punto AP 7220 proporcionan aproximadamente una ganancia de +10dBi que normalmente soporta una mínima tasa de transmisión de datos de 12 Mbps con un 90% disponibilidad para distancias de hasta 760 m en un ambiente urbano con línea de vista LOS.

<u>EFECTO POR OBSTÁCULOS:</u>

Los enlaces de tránsito dependen de tener una línea de vista LOS “limpia”. Un enlace obstruido (por lo general se encuentran en un entorno urbano o suburbano) reduce la tasa de transmisión de datos o lo bloquea completamente.

El uso de un dipolo permite movilizar el punto de acceso AP una distancia corta hacia otro ángulo con la finalidad de tener una mejor visión del otro punto sobre el obstáculo o se puede utilizar una antena auxiliar más potente para poder "penetrar" la obstrucción y poder garantizar un óptimo enlace de tránsito.

LÍMITE VERTICAL DEL BEAMWIDTH DE UNA ANTENA INTEGRADA:

Las antenas integradas del enlace de tránsito se centran en un beamwidth de 3 dB de ±8° con respecto a la horizontal. Hay que asegurarse de que las elevaciones entre los pares AP 7220 están sobre el límite establecido para asegurar el máximo rendimiento Throughput del enlace y evitar caídas de los nodos.

3.5.1.4 FACTORES QUE INCIDEN EN LA INSTALACIÓN DE UN PUNTO DE ACCESO AP 7220

Se requiere de un montaje del AP 7220 en una ubicación adecuada para tener un enlace de acceso óptimo. Los típicos lugares de montaje incluyen postes, paredes, tejados o techos, para la instalación de este equipo hay que considerar los siguientes factores:

- Disponibilidad de una fuente continúa de energía eléctrica que cumpla con las especificaciones del equipo AP 7220.
- Una localización sólida y segura de instalación. El lugar donde se planea realizar el montaje del equipo debería ser:
    - Resistente a condiciones climáticas críticas.
    - Seguro, para evitar daños ya sea por accidentes fortuitos o vandalismo.
    - Adecuado para prevenir daños accidentales, como los causados por los accidentes de tránsito.
- Permiso para montar el punto AP 7220 en la ubicación prevista y acceder a la fuente de energía prevista.

3.5.1.5 FACTORES DE UNA RED DE INFRAESTRUCTURA

Dentro de los factores que se consideran para tener una red de infraestructura óptima, el cliente típicamente plantea sus requerimientos al proveedor para desplegar la red.

Mapas del área geográfica son el método recomendado para describir el área de cobertura y ubicación de equipos. Se debe tener claro el ambiente del despliegue, la densidad de puntos de acceso, densidad de usuarios móviles, aplicaciones y servicios que se desplegarán en la red.

También se debe considerar el ancho de banda a utilizarse, equipos de backup, topología de red.

En la red de backbone la distancia máxima que debe existir entre un punto de acceso AP 7220 y su router NAP asociado debe estar dentro de los 100 m, que es lo que indican las especificaciones de los equipos.

3.5.2 DISEÑO ENFOCADO EN LA ALTA DISPONIBILIDAD

Disponibilidad es la viabilidad de la red tras el fallo de uno o más componentes, es expresada en porcentaje o en "tiempo (minutos) fuera de servicio por año".

Los factores que determinan la disponibilidad de una red inalámbrica Mesh son:

- Fallo de uno o más elementos a lo largo de una ruta de tráfico de la red.

- Resistencia de la red; es decir, la capacidad de la red para redirigir el tráfico a lo largo de caminos alternativos.

A continuación se presenta la disponibilidad de los elementos de una red inalámbrica Mesh:

Tabla XI: Disponibilidad de los Elementos de la Red Mesh

Element	Availability	
	(as %)	(as down time)
Wireless Gateway 7250 (see Note 1)	99.997%	16 min/yr
Network Access Point Router	99.99%	47 min/yr
Wireless AP 7220 @ NAP	single: 99.85% redundant pair 99.9998%	800 min/yr 1 min/yr
Wireless AP 7220	no overlap: 99.85% 50% overlap: 99.92%	800 min/yr 400 min/yr

3.5.2.1 DISPONIBILIDAD DE UN PUNTO DE ACCESO AP 7220

Cuando un usuario móvil que utiliza un dispositivo del estándar 802.11b se conecta a un punto de acceso en la red Mesh y el AP al cual está asociado sufre un daño, inmediatamente se busca una alternativa para conectarse a otro AP.

Para apoyar el acceso de un nodo móvil a través de un punto AP 7220 alternativo, hay que garantizar que las zonas del enlace de acceso tengan superposición en la cobertura de la siguiente manera:

- Si las zonas de cobertura del enlace de acceso se superponen, el nodo móvil se conecta al punto AP 7220 alternativo inmediato.

- Si el nodo móvil no está en una zona de cobertura del enlace de acceso donde existe la superposición, el usuario debe:

    - Aplicar roaming para encontrar y poder conectarse con un punto de acceso AP 7220 alternativo.

    - Esperar que el punto de acceso AP 7220 que está fuera de servicio logre levantar el enlace.

Una zona de superposición donde se involucran dos o más puntos de accesos está afectada por el espaciamiento y por el número de puntos de acceso AP 7220. Por lo tanto para cubrir una zona en su totalidad se requiere un estudio detallado y minucioso sobre el lugar para lograr el mayor espaciamiento entre los puntos de acceso teniendo un mayor número de puntos AP 7220, los cuales no deben estar muy separados ni saturar la red con demasiados puntos de acceso.

<u>DISPONIBILIDAD DE UN PUNTO DE ACCESO AP 7220 @ NAP:</u>

Este punto de acceso es más robusto y por lo tanto está conectado directamente al router NAP, por lo que si el punto de acceso AP@NAP falla entonces todos los demás puntos de acceso AP 7220 conectados hacia este equipo también quedarán fuera de servicio, por tal razón el tráfico es enrutado hacia un punto de acceso AP@NAP alternativo siempre y cuando pueda soportar todo el tráfico que se añade; además, deben utilizar la misma área que se configura en el protocolo OSPF aplicado como enrutamiento.

3.5.2.2 DISPONIBILIDAD DEL ROUTER WIRELESS AP (NAP-R)

Si un router NAP falla y queda inoperativo, todos los puntos de acceso AP 7220@NAP que se conectan directamente a este equipo tampoco funcionarán, por tal razón se debe enrutar el tráfico del punto de acceso hacia un router NAP alternativo.

En una red hay que garantizar al menos dos routers NAP, ya sea que trabajen de manera independiente o que uno funcione de backup y que estén conectados al mismo Wireless Gateway 7250.

3.5.2.3 DISPONIBILIDAD DEL WIRELESS GATEWAY 7250

El modelo del equipo no permite tener una redundancia de la puerta de enlace, por lo que la solución en caso de algún fallo del equipo Gateway 7250 es tener configurado un equipo de repuesto y en caso de falla poder cambiarlo manualmente y poder trabajar con normalidad luego del cambio.

3.5.2.4 DISPONIBILIDAD DE UNA RED DE TRANSPORTE

Los enlaces de la red de transporte conectan:

- Un punto de acceso AP 7220@NAP con su respectivo router NAP.
- Un router NAP conectado a su puerta Wireless Gateway 7250.
- Un Wireless Gateway 7250 conectado al servidor NOSS, a la red de backbone y a la puerta de enlace externa que se conecta hacia el Internet.

Las redes de transporte son muy variables dependiendo del tamaño y el alcance de la red Mesh. El cableado estructurado de la red Mesh involucra un cableado de un punto Ethernet 10/100 BaseT por ejemplo entre un equipo Wireless AP 7220@NAP con su router NAP, así como la utilización de una red de infraestructura con líneas ya sean de cobre o fibra óptica para los equipos de backbone, o enlaces radiales para la conexión entre los puntos de acceso.

El cableado está realizado de tal manera que proporcione rutas alternativas en caso de que algún punto falle y quede fuera de servicio.

3.5.3 DISEÑO ENFOCADO EN EL DESEMPEÑO

El termino desempeño o rendimiento en las redes Mesh es la capacidad de una red para entregar tráfico de manera rápida y eficiente, y se lo puede verificar de tres maneras:

3.5.3.1 CAPACIDAD

La capacidad de la red es la cantidad de tráfico que se puede transmitir simultáneamente a múltiples usuarios. Los siguientes factores limitan la capacidad en una red inalámbrica Mesh, los cuales se detallan en el Anexo 7:

- Tasa de Transmisión de Datos del Enlace de Acceso.
- Capacidad y Rendimiento de la Red Backhaul.

3.5.3.2 RENDIMIENTO

Rendimiento o Throughput es la cantidad de carga útil (payload) que un usuario puede transmitir. Es uno de los factores más críticos que afecta a un usuario que puede variar dependiendo de:

- La aplicación que ejecuta un usuario.
- El número de usuarios que al mismo tiempo acceden a un punto de acceso AP 7220.
- La distancia entre el usuario y el punto de acceso AP 7220.
- La ubicación del punto de acceso AP 7220 dentro de la red.
- La estructura general de la red.

Aunque no se puede controlar las aplicaciones que los usuarios puedan utilizar, un buen diseño puede mejorar el rendimiento de estos planificando:

- Zonas donde existen una mayor concentración de puntos de acceso AP 7220 y donde existen un elevado número de usuarios conectados, permitiendo que cada punto de acceso tome un número reducido de usuarios y no se sature con tráfico.

- Zonas donde existan puntos de acceso AP 7220 con antenas PIFA que permitan delimitar de mejor manera el área de cobertura evitando que exista superposición (overlapping) y por ende evitar que los canales de los enlaces compitan entre sí, y pueda proporcionar mayor rapidez y despliegue en la red.

- Mayor número de puntos de acceso AP 7220@NAP para que conecten puntos de acceso AP 7220 y permitan crear una topología de mayor eficiencia para que fluya el tráfico del usuario con mayor rapidez a través de la red.

- Configurar diferentes canales de frecuencia en los puntos de acceso AP 7220 para apoyar de mejor manera el recurso RF y evitar interferencias, aumentando el ancho de banda a cualquier usuario de la red que lo solicite.

3.5.3.3 LATENCIA

El término Latencia en las redes Mesh se debe a retrasos en la transmisión de paquetes en el enlace de tránsito dentro de la red. La latencia puede resultar de:

- La retransmisión de paquetes retrasados, en la cual cada salto a un punto de acceso AP 7220@NAP presenta retraso debido a que un paquete debe ser recibido antes de que pueda ser retransmitido.
- Una mala programación del enlace de tránsito, debido a que un punto de acceso AP 7220 tiene varios enlaces de tránsito disponibles y si no hay un enrutamiento adecuado se provoca un retraso hasta poder transmitir el paquete. El retraso entre los enlaces de tránsito promedio en una red debe ser máximo de 50 ms.

Para reducir la latencia hay que planificar no más de tres saltos entre el punto de acceso AP 7220 con el punto AP 7220 @NAP asociado.

3.5.4 DISEÑO ENFOCADO EN LA MOVILIDAD

La movilidad es la capacidad del nodo móvil para mantener una conexión en movimiento cuyo punto primordial es que las redes sean contiguas, ya que si no lo son, el usuario tendrá perdida de datos, conexiones fuera de servicio y otros problemas que afectarán el servicio.

Una cobertura para que sea continua, es decir que pueda garantizar la movilidad de los usuarios, exige al menos un 30% la superposición de los puntos de acceso AP 7220 en las zonas de cobertura del enlace de acceso, para evitar zonas muertas que van a restringir la movilidad y poder ofrecer un servicio aceptable a un nodo móvil.

Se puede realizar movilidad a través de redes Mesh diferentes, aplicando roaming a nivel de la puerta de enlace de las redes con los equipos Wireless Gateway 7250.

3.5.5 DISEÑO ENFOCADO EN LA SEGURIDAD

En lo que respecta a la seguridad, hay dos aspectos que deben ser tomados en cuenta al desplegar una red inalámbrica Mesh:

- Seguridad en una red pública "no confiable" (desde equipo Wireless Gateway 7250 hacia el nodo móvil).

Aquí se aplican mecanismos de seguridad en el equipo Gateway 7250 como: túneles IPSec, la autenticación y cifrado, que son incorporados para proteger el tráfico del usuario, el control de tráfico y la gestión del tráfico.

- Seguridad a nivel de Operadores en la red de Infraestructura (desde el equipo Wireless Gateway 7250 hacia el servidor NOSS y puerta de enlace WAN).

La red inalámbrica Mesh supone que la red privada es un entorno confiable en el que los operadores de redes pueden aplicar sus propios mecanismos de seguridad, donde se pueden configurar firewalls y filtros para bloquear puertos, redes públicas y demás puntos que el operador puede considerar peligroso para su red privada.

3.5.6 DISEÑO ENFOCADO EN LA TOPOLOGÍA

El rendimiento y la fiabilidad de una red se basan en la topología de la red. Una red inalámbrica Mesh confiable tiene rutas redundantes y existe superposición de las celdas, lo cual implica una ventaja de estas redes inalámbricas, pero si no está configurado de manera correcta se consumen recursos reduciendo el rendimiento, por tal razón se realiza un balanceo de carga para asegurar que la red Mesh sea eficiente.

A continuación se detallan diferentes topologías para asegurar que la red Mesh sea confiable y tenga un desempeño óptimo:

3.5.6.1 DISEÑO DE TOPOLOGÍA POR RENDIMIENTO

Para poder desarrollar una topología proporcionando el mejor desempeño se debe tener en cuenta lo siguiente:

- Ubicar los puntos de acceso AP 7220@NAP donde la capacidad demandada sea la más alta y la latencia la mínima.
- En ambientes urbanos, los puntos de acceso AP 7220@NAP se deben localizar en las intersecciones donde haya mayor convergencia de puntos o en los límites de la red, permitiendo que estos puntos de acceso puedan visualizar con una mejor eficiencia a los puntos de acceso AP 7220.
- Los AP 7220@NAP deben estar localizados de tal manera que no se puedan ver entre ellos.

La Figura 3-51 muestra una topología correcta basada en los puntos anteriores:

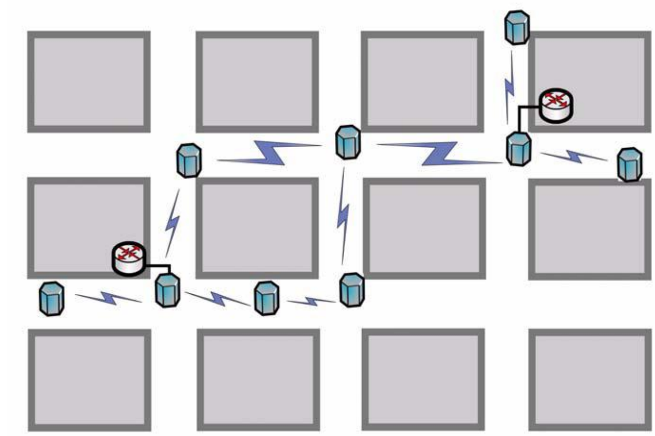


Figura 3-50 Ubicación de puntos de acceso Ap7220 y Ap7220 NAP en un área urbana

Para evitar que en el tráfico de la red se produzca un “Cuello de Botella” hay que tener una distribución adecuada de los puntos de acceso de tal manera que un punto de acceso no debe formar un árbol de red largo ya que no tendrá la capacidad de transmitir a sus puntos derivados el ancho de banda requerido, por tal razón se deben colocar puntos de acceso AP 7220@NAP cercanos a un router NAP para asegurar la capacidad total del tráfico. A continuación se muestra una topología correcta y una topología ineficiente.

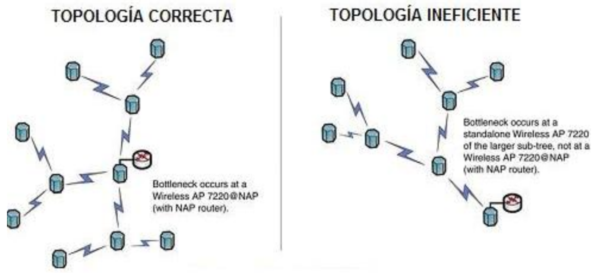


Figura 3-51 Topologías de red basada en Rendimiento para evitar Bottlenecking

A continuación se muestran topologías planteadas de acuerdo a los puntos mencionados, se plantea una topología simple o inicial y una mejorada de la misma.

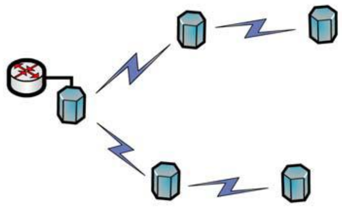


Figura 3-52 Topología de red simple

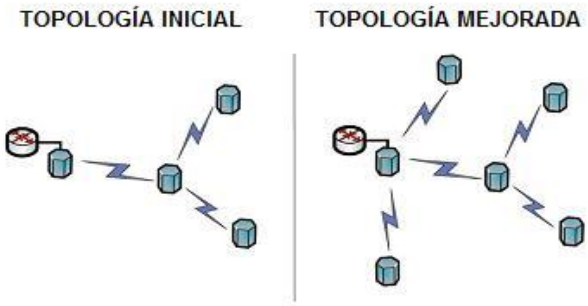


Figura 3-53 Topología de red tipo Estrella

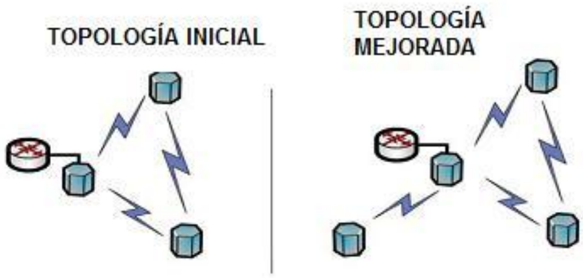


Figura 3-54 Topología de Red tipo Triángulo

Las topologías que se basan en rendimiento tienen como objetivo ofrecer el máximo desempeño de la red sin importar el tamaño final de la red, por tal razón para implementar un mayor número de puntos de acceso se añaden los equipos a continuación del punto de acceso AP@NAP con el objetivo que tengan que realizar el menor número de saltos hacia el router NAP.

3.5.6.2 DISEÑO DE TOPOLOGÍA POR FIABILIDAD

El software de un punto de acceso AP 7220 detecta cuando un nodo falla y automáticamente enruta el tráfico a un nuevo camino que se encuentre a su alrededor. Cuando un nodo se recupera, el software enruta el tráfico a la ruta inicial. Se debe considerar los siguientes puntos a la hora de diseñar una topología con características de fiabilidad:

- Tener los puntos de acceso AP 7220 necesarios para proporcionar la redundancia en el enlace de transito cuando sea requerido.

- Proporcionar redundancia de un enlace de tránsito requiere implementar más enlaces de tránsito, lo cual reduce el rendimiento.

- El camino redundante del enlace de tránsito es más importante para los puntos de acceso AP 7220 que están más cercanos al router NAP, para asegurarse una conexión confiable a la red cableada.

- Asegurarse de que los enlaces redundantes son realmente redundantes; es decir, asegurarse que estos enlaces de tránsito no sean utilizados para transmitir tráfico regular, o que no se encuentren inactivos (ya sea por bloqueado o falla de la potencia de señal) para que sean utilizados en cualquier momento en caso de fallas de los enlaces principales.

A continuación se presenta una topología para el cual tenemos una alta fiabilidad pero con un rendimiento promedio, mediante el uso de topologías de anillo:

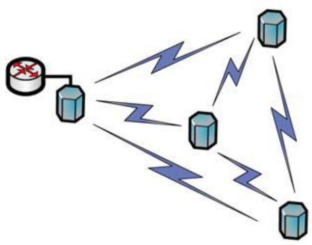


Figura 3-55 Topología de red con alta fiabilidad

En caso de una falla en algún nodo, existe un camino redundante para llegar a cualquier punto de acceso, sin verse afectado los demás nodos:

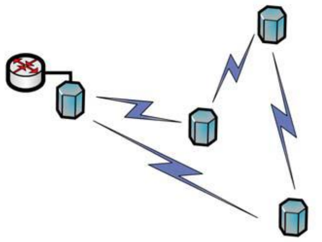


Figura 3-56 Topología de red con una buena fiabilidad y rendimiento

3.6 MÉTRICAS PARA EVALUAR EL DESEMPEÑO DE LA RED

Una red Mesh debe ser capaz de transportar el tráfico de los usuarios hasta el destino indicado. El desempeño puede afectar el nivel de satisfacción de los usuarios ya que estos pueden requerir altas tasas de transmisión con el menor retardo posible ya sea audio, video, datos, etc. Por lo tanto, es necesario evaluar el desempeño de la red a través de diferentes métricas dentro de las cuales encontramos:

3.6.1 CAUDAL EFICAZ

El caudal se define como la cantidad de información que ha llegado exitosamente al receptor. La siguiente ecuación muestra como se realiza el cálculo que ofrece un valor en porcentaje, donde *PR* son los paquetes totales recibidos y *PT* son los paquetes totales enviados.

$$C = (PR/PT) \times 100$$

3.6.2 RETARDO

El retardo se define como el tiempo que transcurre desde que un paquete es enviado por un nodo fuente a través del medio de comunicación hasta que éste es recibido por la estación destino y es medido en segundos; la ecuación muestra el cálculo, donde *TR* es el tiempo de transmisión del paquete y *TT* es el tiempo en el que se recibe el paquete.

$$R = TR - TT$$

3.6.3 PÉRDIDA DE PAQUETES

La pérdida de paquetes se define como la cantidad de paquetes que se enviaron menos la cantidad de paquetes que se recibieron. Se verifica en términos de porcentaje, donde PT es la cantidad de paquetes enviados y PR es la cantidad de paquetes recibidos.

$$PP = ((PT - PR)/ PT) \times 100$$

3.6.4 VARIACIÓN EN EL RETARDO

La variación de retardo o Jitter se define como la variación en el tiempo de llegada de los paquetes, puede ser causado por congestión en la red o por las diferentes rutas que siguen los paquetes hasta llegar a su destino. El jitter se puede calcular con la ecuación que se detalla a continuación, donde *RP* es el retardo promedio, RM es el retardo máximo y Rm es el retardo mínimo.

$$J = ((RM - RP) + (RP - Rm)) / 2$$

3.7 SOPORTE DE CALIDAD DE SERVICIO QoS EN EQUIPOS NORTEL

Dentro de las características que presentan los equipos Nortel, la calidad de servicio QoS es uno de los puntos más importantes, ya que asegura que la red trabaje sin problemas, los parámetros de configuración se realizan en diferentes equipos con la finalidad de ofrecer al usuario final el servicio de voz, video y datos de manera óptima.

3.7.1 CLASIFICACIÓN DE TRÁFICO

El soporte de calidad de servicio requiere el uso de servicios diferenciados DiffServ que tienen como objetivo identificar el tráfico en pocas clases mediante la clasificación de paquetes utilizando mecanismos de encolamiento (queing) para dar prioridad a los paquetes con la finalidad de mejorar considerablemente el problema de latencia.

Además se marcan los paquetes mediante el valor DSCP (Differentiated Services Code Point) que hace referencia al segundo byte en la cabecera de los paquetes IP y es utilizado para diferenciar el servicio de comunicación. Los bits utilizados para el marcado DSCP son del 0 al 5, de los cuales originalmente los tres primeros bits son identificados para el tipo de servicio DiffServ y los bits 6 y 7 no tienen uso. A continuación se muestra la identificación de los bits para DSCP dentro de la cabecera IP y la clase de servicio con su respectiva clase de servicio CS:

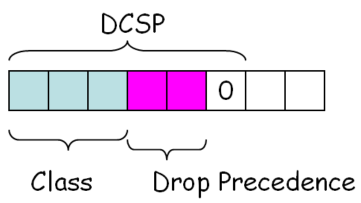


Figura 3-57 Identificación de los bits de marcado DSCP en la cabecera IP

Tabla XII: Tipo de servicio basado en 3 bits del marcado DSCP

CSx	Significado histórico	Uso generalizado
111	Network Control	Tráfico de control (ej: routing)
110	Internetwork Control	
101	CRITIC/ECP	Voz
100	Flash Override	Vconf., streaming
011	Flash	Call signaling
010	Immediate	Libres para clasificar tráfico de datos
001	Priority	
000	Routine	*default*

Adicional, los bits que faltan (3 y 4) ayudan a definir la clase AF (Assured Forwarding) o Envío Asegurado con el cual se puede identificar 4 clases donde cada una tiene una reserva en cada nodo (Ancho de Banda BW o espacio del búfer) y cada clase tiene 3 probabilidades de descarte (*drop*):

Tabla XIII: Tipo de servicio DiffServ basado en el marcado DSCP

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010 AF11	010010 AF21	011010 AF31	100010 AF41
Medium	001100 AF12	010100 AF 22	011100 AF32	100100 AF42
High	001110 AF13	010110 AF23	011110 AF33	100110 AF43

Se especifican cuatro categorías para el acceso de una red Mesh:

- AC_VO (voice)
- AC_VI (video)
- AC_BE (best effort)
- AC_BK (background)

Las tramas de los clientes Mesh del estándar 802.11 incluyen un control de calidad de servicio que viene especificado en la norma 802.11 d que se encarga de la revisión de la prioridad de la trama. A continuación se presenta la Tabla XIV donde se detalla el servicio de marcado DSCP para la clasificación del tráfico:

Tabla XIV: Clasificación de tráfico IP-DSCP

802.1D	Nombre IP-DSCP	Valor IP-DSCP	Tipo de Paquete
7	CS7	111000	Voice
6	CS6	110000	Voice
5	CS5	101000	Video
4	CS4	100000	Video
3	CS3	011000	Best Effort
0	CS0	000000	Best Effort
2	CS2	010000	Background
1	CS1	001000	Background

3.7.2 AUTENTICACIÓN DE UN USUARIO AL SERVIDOR RADIUS

El proceso de autenticación de un usuario dentro de una red Mesh es un punto muy importante, ya que constituye el primer paso para que un usuario pueda iniciar sesión y pueda hacer uso del servicio.

El servidor Radius hace uso del túnel para asignar un ID al usuario que se conoce como "Tunnel-Assigment-ID" que es el encargado de transferir la petición de autenticación al punto de acceso AP a través del mensaje de autenticación de respuesta enviado por el servidor RADIUS cuando un nuevo cliente es asociado.

Los usuarios se asignan a una de las cuatro clases de tráfico que se utilizan en las redes Mesh, donde el servidor RADIUS puede fijar a cualquiera de los tres valores definidos:

- Voz -> AC_Vo(ice)
- Video -> AC_Vi(deo)
- Datos -> AC_BK(ackground)

Cualquier otro valor o si el atributo no es devuelto, el resultado se lo identifica como 'desconocido':

- Desconocido -> AC_Be(stEffort)

Para conocer el estado de disponibilidad de un usuario se lo puede identificar por medio de: informes MAC / IP / Estado / Tipo / SSID.

3.7.3 REDES MESH SOBRE EL ENLACE DE ACCESO

En el enlace de acceso se marcan los paquetes con un valor AC (clase de acceso de una red mesh). Para los paquetes de aplicación existen cuatro colas independientes, una por clase de acceso AC, con resolución interna de colisiones para seleccionar las tramas con prioridad más alta para transmitir.

Los mecanismos de colisión se basan en dos parámetros:

- Minimum inter-frame space (AIFSN)
- Contention Window (CW)

Cabe recalcar que permiten mapeo externo para colas de video y de voz en equipos que no soporten redes Mesh. A continuación se muestra los cuatros servicios de manera independiente para ser transmitidos hacia un dispositivo de un usuario:

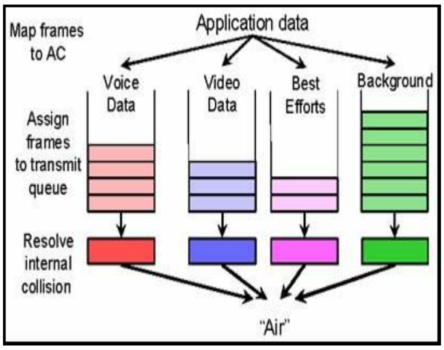


Figura 3-58 Redes Mesh sobre el Enlace de Acceso

3.7.4 PRIORIDAD MÚLTIPLE EN COLA (QUEUE)

En lo que respecta a Nortel se han identificado diferentes clases de servicio, que se clasifican según el tipo de tráfico que se transmite y que se identifican por medio del marcado DSCP.

A continuación se presenta una tabla detallando las diferentes clases de servicio con su respectiva aplicación y detallando el número lógico que se encuentra en la cola (queue) que indica su prioridad cuando se transmiten varios servicios en un tiempo determinado:

Tabla XV: Clases de Servicio de Nortel y prioridad de cola

Categoria del Tráfico	Clase de Servicio	Aplicación	DSCP	Numero Logico en la Cola	Prioridad
Control de Red	Critical	Critical Heartbeats	CS7	1	Pre-emptive
	Red	Routing	CS6	2	
Interactivo	Premium	IP Telephony	CS5		Alta
	Platinum	Video Conferencing	CS4	3	Media
Respuesta	Gold	Streaming Media	CS3		Baja
	Silver	Client/Server	CS2	4	
Tiempo	Bronze	Store and Forward	CS1		
	Standard	Best Effort	CS0		

De acuerdo a la tabla podemos identificar lo siguiente respecto a las clases de servicio de Nortel:

- El número con mayor prioridad en la cola es el número 1 y el de menor el número 4.

- El tráfico con mayor prioridad es de Control de Red teniendo una clase de servicio Crítica que es la más alta, mientras que el Tiempo es la categoría de menor prioridad que tiene las clases de servicio de Bronce y Estándar.

- Si se observan las aplicaciones, los servicios para el cliente que tienen mayor prioridad es de voz como lo es VoIP sobre el servicio de datos como lo es una aplicación cliente/servidor.

- El tráfico de Background (desconocido) o Best Effort se le asigna una prioridad tipo Estándar.

3.7.5 PROGRAMADOR DE QoS EN EL ENLACE DE TRÁNSITO

El tamaño del slot del Enlace de Tránsito dinámico permite reducir el retardo punto a punto cuando es detectado un retardo en el tráfico. Por esta razón se adapta times slot sobre la base de los enlaces y sobre la congestión.

El tamaño del slot dinámico puede tener una duración de 25 a 50 ms, a menos que los tamaños de los slots fijos tengan un tiempo que varíe entre los 30 a 50 ms.

Si múltiples time slots tienen un retardo mayor al indicado entonces se congestionan entre sí, causando que el programador aumente el tamaño para aquel punto.

De esta manera se reducirá el jitter en el enlace de tránsito y se evitará congestión en los puntos donde existe mayor tráfico.

3.8 TOPOLOGÍA LÓGICA DE LA RED A DESARROLLAR

TOPOLOGÍA ACTUAL DE LA RED EN LA FIEC

La FIEC actualmente tiene implementada una topología de red en estrella, la misma que es híbrida puesto que mezcla fibra óptica y tecnología inalámbrica, donde la red inalámbrica cubre aproximadamente el 80% del total del área de la facultad, para lo cual se utilizan 15 puntos de acceso de marca Enterasys y Cisco.

A continuación se presenta una vista aérea de la Facultad con la ubicación de los puntos de acceso y la cobertura Wifi desplegada actualmente:

Figura 3-59 Cobertura de la red inalámbrica actual de la FIEC

Donde,

Los puntos de acceso de la marca Cisco se representan con el símbolo: ■

Los puntos de acceso de la marca Enterasys se representan con el símbolo: ▲

La desventaja que se nota en la red implementada en la FIEC es que no cubre por completo el 100% del área de la facultad, además, que no permite mucha movilidad a los usuarios.

3.8.1 UBICACIÓN DE EQUIPOS

Como se definió para el desarrollo del diseño y simulación de la red mesh para la FIEC se utilizarán los equipos de NORTEL Networks.

- Servidor NOSS
- Wireless Gateway 7250
- Router NAP
- AP@NAP

3.8.1.1 PUERTA DE ENLACE WIRELESS GATEWAY 7250

El servidor NOSS, el Wireless Gateway 7250, el Router NAP y el punto de acceso AP@NAP que pertenecen al backbone Mesh, deben de estar ubicados en el bloque de los laboratorios de computación, ya que en este lugar se encuentra el enlace WAN, los servidores y administradores de la red.

A continuación se presenta el bloque de laboratorios donde deben ir los equipos de backbone:

Figura 3-60 Bloque de Laboratorios de la FIEC

3.8.1.2 PUNTOS DE ACCESO AP 7220

Para la red mesh de la FIEC se utilizará los puntos de acceso AP7220, los cuales se tienen que ubicar en sitios estratégicos en base a parámetros de propagación para cubrir toda el área de la Facultad.

Cabe recalcar que algunos APs no tendrán línea de vista para realizar el enlace de tránsito entre ellos, para solucionar este inconveniente se utilizará antenas auxiliares (Figura 3-61), las cuales son recomendadas por el proveedor y servirán para evitar pérdidas de comunicación y aumentar la redundancia de la red, el cual es uno de los objetivos de la solución mesh que se plantea.

Figura 3-61 Implementación de las antenas auxiliares

A continuación se presenta una vista aérea de la ubicación de los puntos de acceso incluyendo el punto de acceso AP@NAP donde también se encontrarán los equipos Wireless Gateway 7250 y el router NAP:

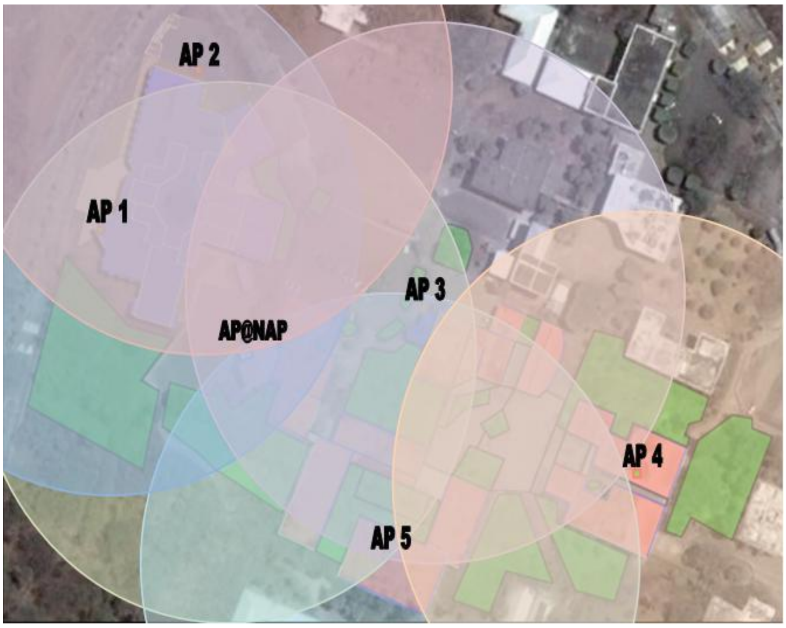


Figura 3-62 Diseño de cobertura de los puntos de acceso AP 7220 para la red Mesh de la FIEC

Las distancias entre cada uno de los APs que se muestran en la Figura 3-62 se detallan a continuación en la Tabla XVI, estás distancias se las definió basándose en los parámetros establecidos por el proveedor para exteriores en condiciones ideales de un ambiente Suburbano con LOS, para asegurar que el enlace de tránsito tenga su máximo rendimiento está comprobado que la distancia máxima entre APs es de 200 metros.

Tabla XVI: Distancias entre los puntos de acceso AP 7220 expresada en metros

	AP NAP	AP1	AP2	AP3	AP4	AP5
AP NAP		73.98	110.97	86.31	178.78	104.81
AP1	73.98		73.98	141.8	246.6	178.8
AP2	110.97	73.98		135.63	252.77	203.45
AP3	86.31	141.8	135.63		117.14	98.64
AP4	178.78	246.6	252.77	117.14		110.97
AP5	104.81	178.8	203.45	98.64	110.97	

En la Tabla XVI se nota que las distancias entre los puntos de acceso AP1 y AP4, AP2 y AP4, AP2 y AP5 son mayores a los 200 metros estimados para asegurar un enlace de tránsito óptimo. Esto no constituye un inconveniente ya que la topología de red facilita que los puntos de acceso estén interconectados por dos saltos, lo cual está dentro de las características de los equipos y facilita el despliegue e interoperabilidad de la red.

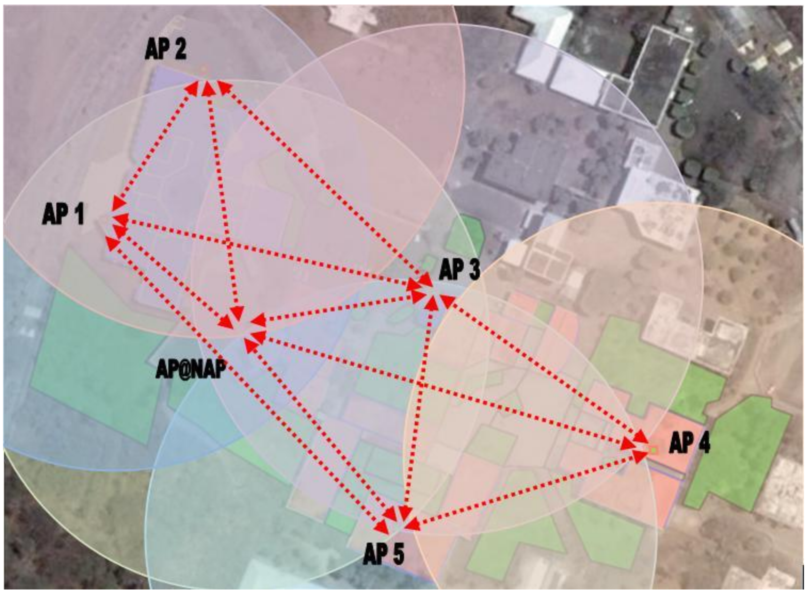


Figura 3-63 Enlaces de tránsito óptimos de la red mesh

De acuerdo a la ubicación de los APs y a los enlaces de tránsito que se logro establecer se nota que la topología del diseño se basa en el rendimiento de la red. Así se asegura el máximo tráfico en toda la red y evita que se cree una topología con subárboles largos y por ende evita la creación de cuellos de botella (bottlenecks) debido a la saturación que se puede formar en algún punto de acceso debido a un mal diseño. En la siguiente figura se presenta la topología empleada para la red de la facultad:

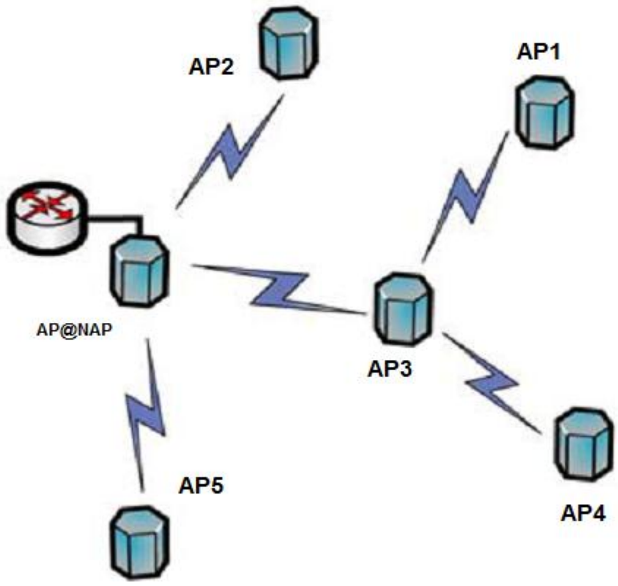


Figura 3-64 Topología de red Mesh a implementarse en la FIEC

<u>UBICACIÓN DE LOS APS DE NORTEL NETWORKS</u>

A continuación se mostrará los lugares de la FIEC donde deberían ir los APs 7220.

AP1

Se debe ubicar en la parte del frente del edificio central de la FIEC, siendo la primera adyacencia del AP@NAP. En la Figura 3-65 se muestra la ubicación del punto de acceso.

Figura 3-65 Ubicación del AP1

AP2

El segundo punto de acceso debe estar ubicado en sobre bloque de la parte posterior izquierda del edificio central de la FIEC. En la Figura 3-66 se muestra el sector mencionado como ideal para ubicar el AP2.

Figura 3-66 Ubicación del AP2

AP3

El tercer punto de acceso en instalarse estará ubicado en el poste de alumbrado eléctrico que se encuentra en el parqueadero cercano al antiguo edificio de profesores de la Facultad. La Figura 3-67 muestra el sector mencionado.

Figura 3-67 Ubicación del AP3

AP4

El cuarto punto de acceso 7220 se debe ubicar en el bloque de aulas de la Facultad, en el centro de la parte superior del bloque mencionado. La Figura 3-68 muestra el lugar planteado.

Figura 3-68 Ubicación del AP4

AP5

El quinto AP7220 debe estar ubicado en el centro del bloque donde se encuentran los laboratorios de electrónica y digitales de la Facultad que limita con el ICM. La Figura 3-69 muestra el sitio mencionado.

Figura 3-69 Ubicación del AP5

3.9 DIRECCIONAMIENTO IP PARA LOS EQUIPOS DE BACKBONE Y USUARIOS

El direccionamiento IP se debe realizar de tal manera que sea de fácil comprensión, eficiente y extensible.

Para obtener las características mencionadas dentro del diseño de red Mesh se debe considerar una red clase A no enrutable como por ejemplo la **10.X.X.X**

Para el caso de la computadora que se va a utilizar como Servidor NOSS debe tener al menos una interface Ethernet con la dirección IP **10.4.1.1/24** configurada de manera estática.

De acuerdo a estas características se debe asignar las siguientes direcciones IP para los equipos y elementos que formarán parte de la infraestructura Mesh:

Tabla XVII: Direccionamiento IP de la red Mesh

ELEMENTO	DIRECCIONAMIENTO IP
Servidor NOSSwin	
Radius, DHCP y FTP Server:	10.4.1.1 / 24
Wireless Gateway 7250	
IP de Administración:	10.4.1.2 / 24
IP Privada:	10.4.1.3 / 24
IP Publica:	10.2.1.2 / 24
NAP Router	
Interface hacia el WG 7250:	10.2.1.1 / 24
Interface hacia los AP 7220:	10.1.1.1 / 24
AP@NAP	10.1.1.2 / 24
AP 7220 #1	10.1.1.3 / 24
AP 7220 #2	10.1.1.4 / 24
AP 7220 #3	10.1.1.5 / 24
AP 7220 #4	10.1.1.6 / 24
AP 7220 #5	10.1.1.7 / 24
Usuarios Terminales:	10.8.1.x / 24

Las direcciones pueden ser modificadas de acuerdo a los requerimientos que se presenten en el despliegue.

En caso de cambiar el direccionamiento IP de los puntos de acceso, se lo realizar en el servidor NOSS modificando el archivo **dhcpd.conf** y en el pool de direcciones configurado en el Wireless Gateway 7250.

Cabe recalcar que el protocolo de enrutamiento que emplean los equipos mesh de Nortel es OSPF, el cual es configurado tanto en el

Wireless Gateway 7250 como en el router NAP-R y la ruta por defecto es **10.0.0.0**

3.10 DIAGRAMA DE LA RED MESH PARA LA FIEC EN EL CAMPUS ESPOL

En el diseño planteado no se considera equipos de backup para el Wireless Gateway 7250 ni para el router NAP, puesto que la red no es compleja, debido a la poca cantidad de usuarios y recursos que demandaran los mismos a la red Mesh, y al diseño de topología que asegura que no sufrirá saturación de ancho de banda por mal enrutamiento.

En caso de existir alguna falla en algún punto de acceso por diversos factores y exista la necesidad de reemplazarlo, no habría problema alguno, puesto que la red se adaptaría a la baja sufrida y el personal de soporte de la FIEC cambiaría sin inconvenientes el equipo defectuoso.

A continuación se presenta un diagrama de red propuesto para la FIEC, donde se detalla de mejor manera la tabla de direccionamiento IP que se detalló en el punto anterior, la topología de los puntos de acceso y los usuarios finales con el SSID a engancharse para tener el servicio:

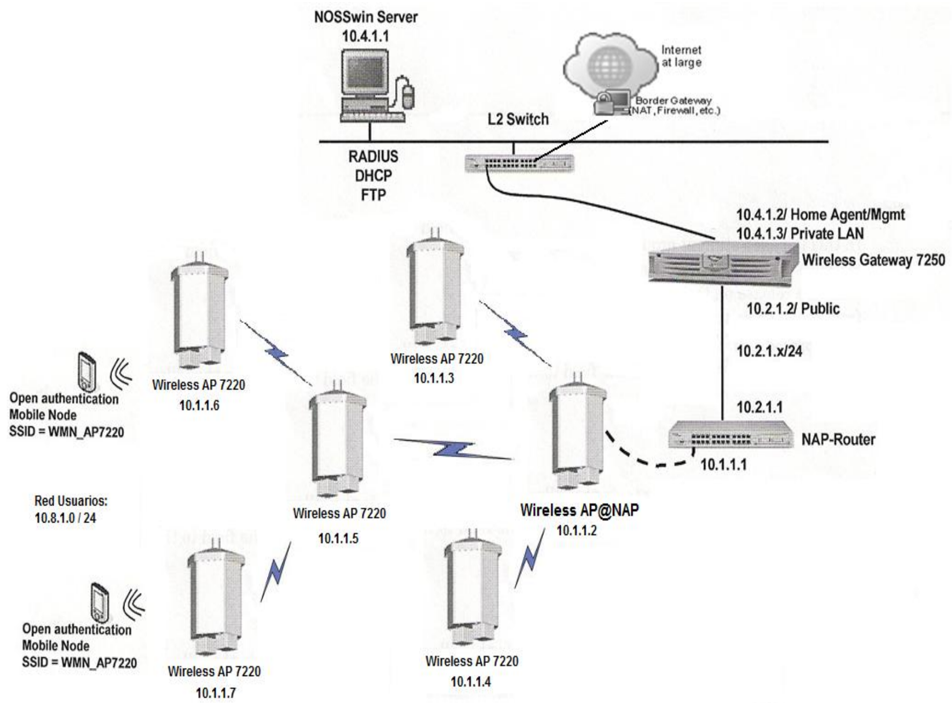


Figura 3-70 Diagrama del diseño propuesto para la red Mesh de la FIEC

A continuación se detalla un análisis del presupuesto para implementar la red mesh en la FIEC de acuerdo al diseño planteado de 6 puntos de acceso AP7220, el cual tiene un margen de error del 15% de lo que podría ser el presupuesto final.

COSTOS DE EQUIPOS:

Para los equipos de Nortel que se utiliza en la solución se tiene una cotización que se muestra en el Anexo K donde se detalla el kit y las respectivas licencias que se necesitan para cada equipo.

En la siguiente tabla se muestra la cantidad de equipos y el precio total en dólares que se necesita para obtener los equipos de la solución mesh para la FIEC:

Tabla XVIII: Lista de precio de equipos utilizados en el diseño de la red Mesh

EQUIPO	MARCA	PRECIO UNITARIO	CANTIDAD	PRECIO TOTAL
Wireless Gateway 7250 Dual 10/100 Ethernet LAN Ports	NORTEL	7,000.00	1	7,000.00
Nortel VPN Router 1100, 5 tunnels, single 10/100 Enet	NORTEL	1,499.00	1	1,499.00
Wireless AP7220 with Co-linear Antenna	NORTEL	3,500.00	6	21,000.00
Router Cisco 871	CISCO	390.00	1	390.00
Switch TPLink 8 Puertos	TPLINK	12.00	1	12.00
SERVIDOR	S/N	426.00	1	426.00
			TOTAL	30,327.00

COSTOS DE INFRAESTRUCTURA:

Dentro de la infraestructura se considera los costos por obras civiles., en lo que respecta a los equipo del backbone mesh no se necesita realizar instalaciones adicionales debido que estarían donde se encuentran los equipos del backbone actual. Para los puntos de acceso se necesita ubicar mástiles de entre 3 y 5 metros.

A continuación se presenta una tabla con los costos por instalación de los puntos de acceso:

Tabla XIX: Costo por instalación de los puntos de acceso

MATERIAL	PRECIO UNITARIO	CANTIDAD	PRECIO TOTAL
Mástil	40.00	6.00	240.00
Abrazaderas	3.30	6.00	19.80
		TOTAL	$ 259.80

COSTOS POR OPERACIÓN

Luego de la implementación de la red se debe consideran los costos de operación, en el cual se encuentra el pago mensual al proveedor de Internet. La recomendación para el servicio, considerando el número de estudiantes y de aplicaciones a utilizar dentro de la red mesh, es contratar un ancho de banda de 2Mbps para asegurar que el servicio no sufra intermitencias ni lentitud.

CAPITULO 4

4. ANALISIS DE PROPAGACION Y COBERTURA MEDIANTE EL USO DEL PLANNER SIMULATOR PARA LA FIEC

4.1 PLANNER SIMULATOR

El uso de un software de aplicación permite realizar un análisis de propagación y comunicación de enlaces en una red inalámbrica Mesh, para lo cual Nortel ofrece dos herramientas conocidas como:

- Planner
- Link Calculator

El concepto que se utiliza para desarrollar un demo de una red Mesh es la aplicación del estándar 802.11b para obtener la cobertura del enlace de acceso lo que permite la comunicación entre el punto de acceso y un usuario final móvil, además de la conectividad de los enlaces de tránsito es decir la comunicación entre los puntos de acceso desplegados en la red.

4.1.1 PLANNER

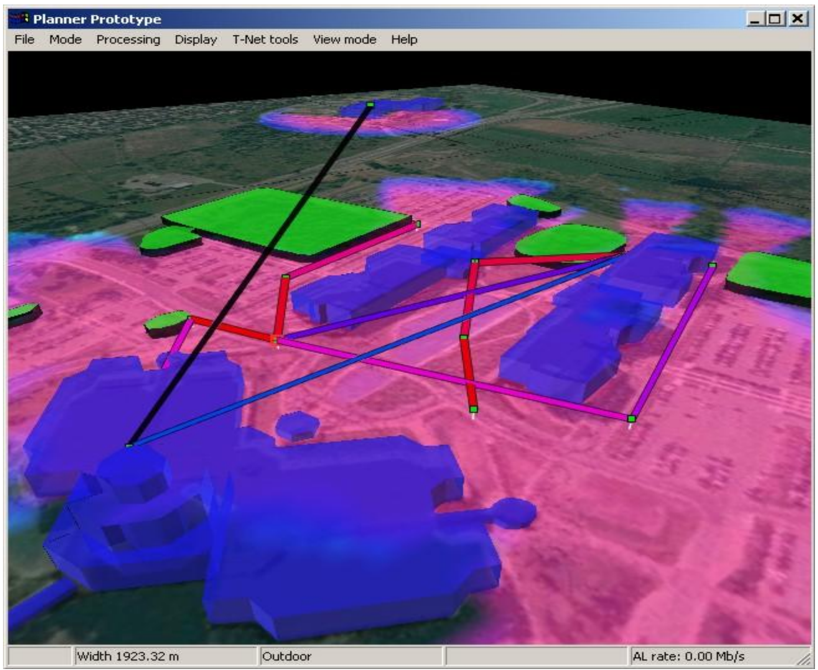


Figura 4-1 Visualización de un Demo en la herramienta Planner

Esta herramienta crea un modelo en 3D para el despliegue de una red y obtiene el área de cobertura empleando conceptos de propagación ideales para el enlace de accesso y conectividad entre los puntos de acceso.

El propósito de esta herramienta es estimar cuantos puntos de acceso AP 7220 se necesitan para cubrir el área donde se plantea implementar la red, seleccionando la mejor ubicación en base a criterios geográficos y de propagación.

La limitación del Planner se debe a que no hay facilidad para el uso de antenas auxiliares, para lo cual se utiliza otra herramienta conocida como Link Calculator.

4.1.2 LINK CALCULATOR

Link Calculator es una herramienta implementada en una hoja de cálculo de Excel que surge como un complemento para el programa Planner, se enfoca en el análisis de los diferentes casos de enlaces de tránsito que se pueden presentar en el despliegue de una red.

El propósito del Link Calculator es extender la funcionalidad del Planner proporcionando la información para configuración de los enlaces de tránsito con antenas auxiliares.

Además se puede analizar el rendimiento tanto del enlace de tránsito como del enlace de acceso expresado en la tasa de datos en Mbps con respecto al rango de distancia expresado en Kilómetros.

La limitación que tiene la herramienta es que realiza un análisis de propagación simple donde se emplean los modelos matemáticos, se ingresan los datos para que sean calculados y se obtiene un resultado único ya que no es un programa Multimedia.

A continuación se presenta la ventana en donde se ingresan los parámetros y se obtienen los resultados:

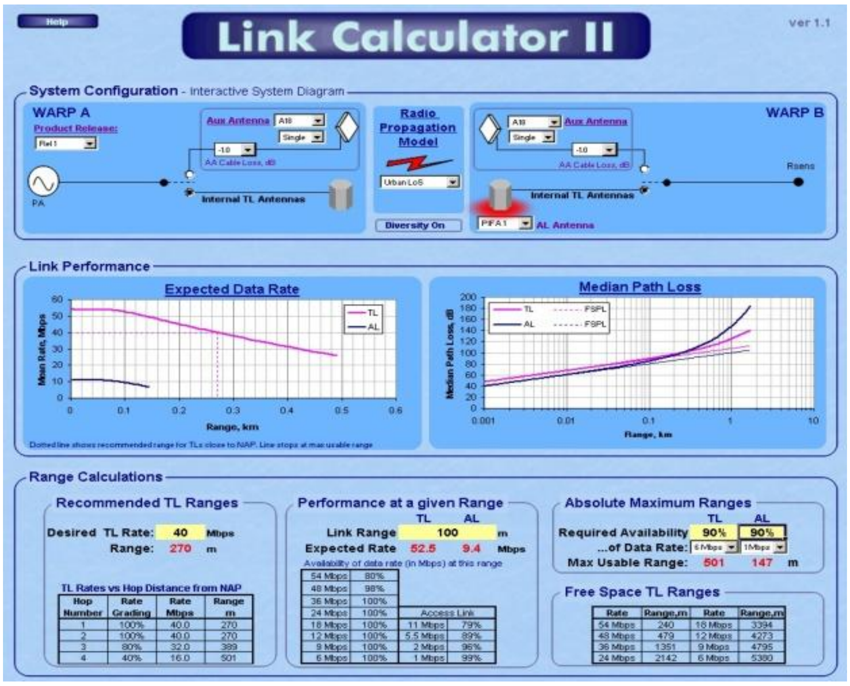


Figura 4-2 Link Calculator II

4.2 ELEMENTOS Y MEDICIONES NECESARIAS PARA EL USO DEL SIMULADOR

El programa Planner es un producto de Nortel que emplea modelo MMPM (Multimedia Propagation Model) el cual es capaz de mostrar modelos de enlaces dependiendo de los ambientes y la atenuación que tengan los diferentes objetos como por ejemplo paredes o árboles.

En la Tabla XX se presentan las diferentes características de cada ambiente y el tipo de atenuación de los objetos con la finalidad de tenerlos presentes al momento de desplegar la red. Los diferentes valores de atenuación se expresan en decibelios por metro:

Tabla XX: Atenuación del Enlace AL y TL en diferentes ambientes

AMBIENTE	**ATENUACION**	
	Enlace de Acceso	**Enlace de Tránsito**
Enlace Limpio	0 dB/m	0 dB/m
LOS Urbana	0.048 dB/m	0.017 dB/m
Indoor Abierto	0.22 dB/m	0.22 dB/m
Indoor Saturado	0.62 dB/m	0.62 dB/m
Vegetación	1.0 dB/m	2.0 dB/m

En un ***enlace limpio*** no hay presencia de obstrucciones entre el transmisor y el receptor.

En un ambiente con ***línea de vista en una área urbana***, tenemos LOS entre el transmisor y el receptor, donde los puntos de acceso están montados en promedio de 6 metros de altura sobre las calles.

En un ambiente ***indoor abierto*** tenemos espacios internos con techos muy altos sin obstáculos, en estos casos tenemos como ejemplos los centros comerciales y aeropuertos.

En un ambiente ***indoor saturado*** tenemos espacios con techos bajos y por lo general hay particiones internas donde no tenemos línea de propagación, es el caso de las oficinas.

La ***vegetación*** incluye todo tipo de arboles con diferentes tipos de altura, los cuales afectan y obstaculizan la línea de vista.

En lo que se refiere a edificaciones tenemos diferentes tipos, dependiendo el tipo de material ya sea que obstaculiza, refleja o refracta el enlace que se está transmitiendo. A continuación se presenta la Tabla XXI que indica el nivel de atenuación dependiendo el tipo de edificación:

Tabla XXI: Atenuación de acuerdo al material utilizado en la Edificación

Tipo de Edificación	**dB**
Aire	0
Pared con Ventanas	6.9
Pared sin Ventanas	15
Paredes Metálicas o Bloquean Luz del Sol	30

De acuerdo a la tabla anterior, el último tipo de edificación se refiere a construcciones con paredes muy gruesas o paredes metálicas. Otro tipo de ejemplo son edificios con paneles recubiertos de acabados metálicos que bloquean la luz hacia el interior y por ende también bloquea las señales de radio.

ENLACE DE ACCESO:

A continuación se muestra un diagrama de un sistema ideal, en la cual se especifica las ganancias y pérdidas que presenta el enlace de acceso:

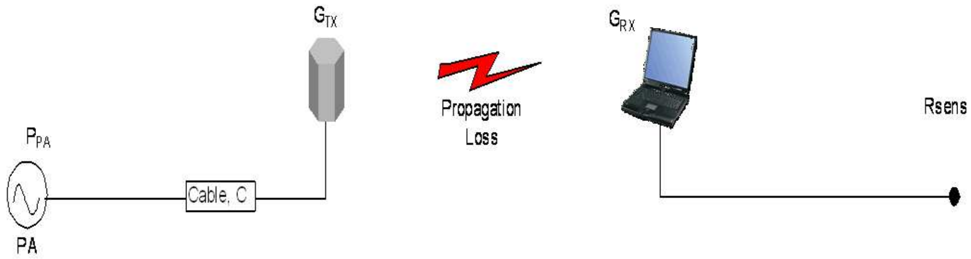


Figura 4-3 Diagrama de un Sistema de Enlace de Acceso

Donde,

PPA	Potencia de salida de PA
C	Cable que conecta la radio con la antena AL. C= -0.5dB
GTX	Ganancia de las antenas
GRX	Ganancia típica de una antena para un terminal. GRX= -3.0dB
LPL	Pérdida de Propagación
RSENS	Sensibilidad de Recepción, varía con la tasa de transmisión.

La Tabla XXII se nota el rendimiento del enlace de Acceso de un equipo terminal de acuerdo al parámetro de la potencia que recibe la radio y tasa de transmisión:

Tabla XXII: Rendimiento de una Radio de Enlace de Acceso

Tasa [Mbps]	PA [dBm]	Sensibilidad de Rx [dBm]
1	18	-92
2	18	-89
5.5	18	-87
11	18	-84

Debido a que un punto de acceso opera en diferentes valores de tasa de transmisión, la pérdida por la trayectoria del enlace L_{PL} tiene que ser calculada en base a la siguiente ecuación:

$$\mathbf{L_{PL} = P_{PA} + C + G_{TX} + G_{RX} - R_{sens}}$$

La pérdida por trayectoria L_{PL} tanto para una antena PIFA como para una antena Co-lineal se expresa en base a la tasa de transmisión, tal como se muestra en la siguiente tabla:

Tabla XXIII: Pérdida por Trayectoria L_{PL} para antenas PIFA y Co-linear en enlace de Acceso

Rate	Ganancia neta: C+Gtx+Grx		L_{PL} [dB]	
Mbps	PIFA	Co-linear	PIFA	Co-linear
1	-4.1	0.1	105.9	110.1
2	-4.1	0.1	102.9	107.1
5.5	-4.1	0.1	100.9	105.1
11	-4.1	0.1	97.9	102.1

Si hacemos un cálculo de la potencia EIRP tenemos lo siguiente:

$$\mathbf{EIRP= P_{PA} + C+ G_{TX}}$$

- Para antenas PIFA: EIRP= 18.9 dBm
- Para antenas Co-linear: EIRP= 23.1 dBm

ENLACE DE TRÁNSITO:

En la Figura 4-4 se muestra un diagrama de un sistema de Enlace de Tránsito, en la cual se especifica las ganancias y pérdidas que se produce en la transmisión y recepción de datos:

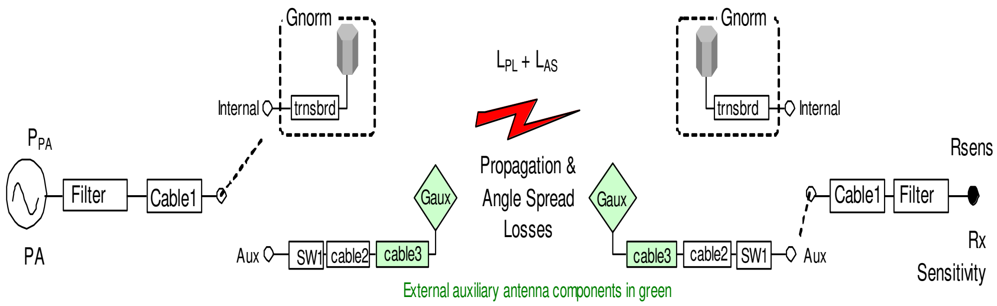


Figura 4-4 Diagrama de un Sistema de Enlace de Tránsito

Donde,

PPA	Potencia de salida de PA
Filtro	
Cable1	Cable que conecta el filtro con el borde de transición

Gnorm — Ganancia de una antena interna y el borde de transición

Gnorm_pk — Ganancia Pico de una antena interna y el borde de transición

Trnsbrd — Borde de transición

ASnorm — Angulo de Propagación para una antena normal

SW1 — Pérdida por conmutación a puerto auxiliar

Cable2 — Cable que conecta el borde de transición con el conector externo

Cable3 — Cable que conecta el conector externo con la antena auxiliar

A continuación se presentan los valores de atenuación establecidos:

Tabla XXIV: Atenuación de los componentes del sistema del Enlace de Tránsito

Parámetro	**dB**
Filtro	-1.6
Cable1	-0.6
Gnorm	8.9
Gnorm_pk	11.5
Asnorm	-1.1
SW1	-1.6
Cable	-0.7

En base a la tasa de transmisión varía el parámetro de potencia transmitida y por ende la potencia recibida en el punto de acceso receptor, tal como se observa en la siguiente tabla:

Tabla XXV: Rendimiento de una Radio de Enlace de Tránsito

Tasa [Mbps]	PA [dBm]	Sensibilidad de Rx [dBm]
6	20	-89
9	20	-88
12	20	-87
18	20	-85
24	20	-81
36	19	-78
48	17	-71
54	14	-68

La pérdida por la trayectoria del enlace L_{PL} tiene que ser calculada en base a la siguiente ecuación:

$$L_{PL} = P_{PA} + G_{NET} - Rsens$$

Donde G_{NET} es la ganancia de ambos transceivers:

- Antenas internas:

$$G_{INT} = Filter + Cable1 + Gnorm - ASnorm$$

- Antenas Auxiliares:

$$G_{EXT} = Filter + cable1 + SW1 + cable2 + cable3 + Gaux - Asaux$$

En base a estas ecuaciones se presenta la siguiente tabla que presenta la ganancia de los transceivers tanto para antenas internas como para antenas externas:

Tabla XXVI: Ganancia de las antenas internas y externas de un Enlace de Tránsito

Ganancia Transceiver [dB]	Propagation	
	Normal	Free Space
G_{INT}	5.6	6.7
G_{EXT} Huber Suhner	6	7.1
G_{EXT} Andrew 18	10.5	12.4

Si hacemos un cálculo de la potencia EIRP tenemos lo siguiente:

- Antenas Internas:

EIRP = PPA + Filter + Cable1 + Gnorm_pk

- Antenas Externas:

EIRP = PPA + Filter + Cable1 + SW1 + cable2 + Cable3 + Gaux

Finalmente podemos calcular la potencia EIRP tanto para antenas internas y como externas, la cual se presenta en la siguiente tabla en base a diferentes tasas de transmisión:

Tabla XXVII: Potencia EIRP para internas y externas de un Enlace de Tránsito

Data Rate	EIRP [dBm]		
[Mbps]	Interna	HuSu	A18
6	29.3	27.1	32.4
9	29.3	27.1	32.4
12	29.3	27.1	32.4
18	29.3	27.1	32.4
24	29.3	27.1	32.4
36	28.3	26.1	31.4
48	26.3	24.1	29.4
54	23.3	21.1	26.4

4.3 IMAGEN DEL ÁREA GEOGRÁFICA DE ESTUDIO

Como se mencionó en el capitulo anterior la FIEC tiene un área de aproximadamente 90000m^2. Tiene laboratorios, bares, zonas de distracción, bloques de aulas, edificios y aéreas verdes.

A continuación se muestra la imagen a utilizar en el planner para proceder con la simulación.

Figura 4-5 Imagen a utilizar en el planner

4.4 PLANEAMIENTO

Para obtener una simulación apegada a la realidad se debe seguir los siguientes pasos.

- **Primero,** se debe escoger una imagen donde se muestre una vista aérea perpendicular a la superficie donde se plantea desarrollar la red mesh (Figura 4-5), para luego importarla al Planner (Figura 4-7) especificando en metros el ancho del área de estudio.

La imagen debe de tener formato **.jpg,** en el caso de la FIEC el ancho del área de estudio es de 325 metros.

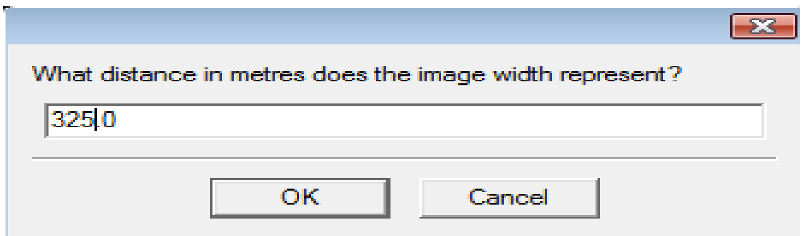


Figura 4-6 Ingreso del ancho real del área de estudio en el Planner

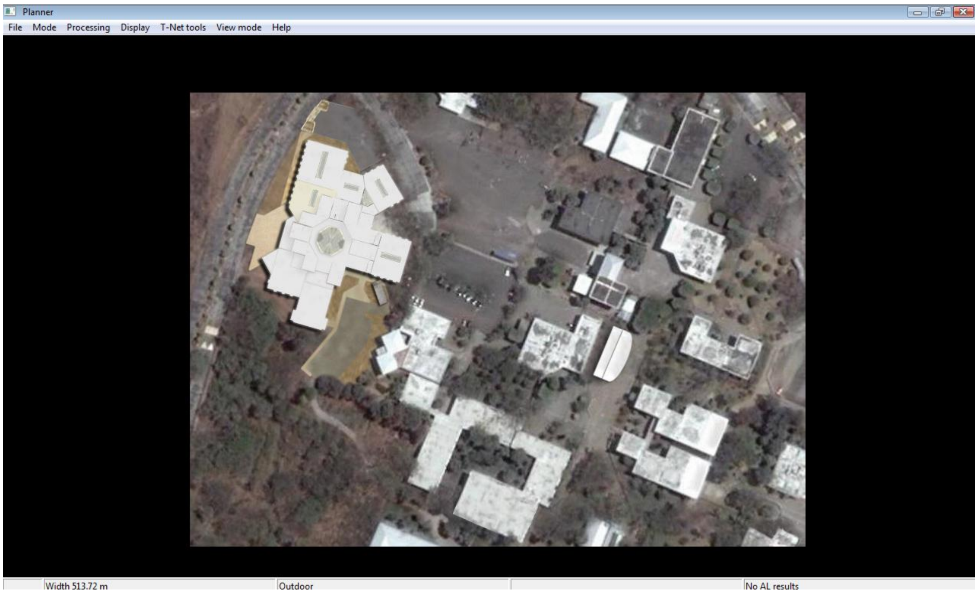


Figura 4-7 Ingreso del plano de la Facultad en el Planner Simulator

- **Segundo,** se sectoriza la imagen con ayuda de colores tanto para aéreas (edificios, aéreas verdes, coliseos) como para perímetros (paredes de cemento, vidrio o metal) detallados en la Tabla XXVI. Además se les designa la altura a cada área definida en la imagen.

Tabla XXVIII: Colores del planner para sectorizar las áreas de estudio

Ambiente	Identificación en el Planner	Boundary Borde	Identificación en el Planner
Area Verde	Verde	Limpio	Negro
Outdoor	Gris	Pared con Ventana	Azul
Indoor Abierto	Azul	Pared sin Ventana	Gris
Indoor Recargado	Rojo	Bloqueo Luz Solar	Rojo

- **Tercero,** se ubican los puntos de acceso AP 7220 y el AP@NAP indicando la altura a la que deben instalar.

- **Finalmente,** se procesa la información en donde se mostrará el área de cobertura en base a una gama de colores que indican la calidad del enlace de acceso basándose en la tasa de transmisión:

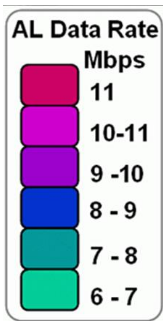


Figura 4-8 Tasa de Datos para el Enlace de Acceso en el Planner

- **Además,** se puede analizar la conectividad entre los puntos de acceso, ya que el programa tiene la opción de graficar la línea de vista LOS entre los equipos, mostrándolas en diferentes tipos de colores que califican la calidad del enlace de Tránsito basándose en la tasa de ancho de banda que pueden transmitir:

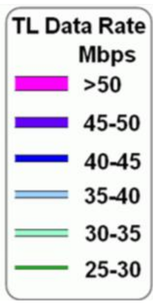


Figura 4-9 Tasa de Datos para el Enlace de Tránsito en el Planner

De acuerdo a los resultados que se obtengan de los enlaces de Acceso y de Tránsito se puede modificar los datos ingresados, como reubicación de equipos o añadir equipos adicionales que permitan cumplir con nuestras expectativas de despliegue de la red.

4.5 MODELAMIENTO: DEFINICIÓN DE AMBIENTES DE ZONAS DE PROPAGACIÓN

En la definición de los ambientes en el Planner, se debe identificar cada unos de los sitios que forman parte de la Facultad de Ingeniería en Electricidad y Computación.

A continuación se detallan los diferentes ambientes que se deben considerar para realizar el despliegue en el simulador:

- Edificio inteligente
- Auditorio
- Aulas de clase
- Laboratorios de computación
- Comedor
- Parqueaderos
- Áreas Verdes

El programa de simulación tiene identificado con diferentes colores cada uno de los posibles ambientes, así como de qué material u objeto están hechos las paredes o límites.

A continuación se presentan dos tablas, la primera detalla la identificación del color para los diferentes ambientes que se pueden presentar (Tabla XXVII); y, la segunda (Tabla XXVIII) detalla el material del cual está formado las paredes de la edificación:

Tabla XXIX: Identificación de Ambientes en el Planner Simulator

Ambiente	Identificación en el Planner
Area Verde	Verde
Outdoor	Gris
Indoor Abierto	Azul
Indoor Recargado	Rojo

Tabla XXX: Identificación de Bordes de Ambientes en el Planner Simulator

Boundary Borde	Identificación en el Planner
Limpio	Negro
Pared con Ventana	Azul
Pared sin Ventana	Gris
Bloqueo Luz Solar	Rojo

En la FIEC se encuentran varios tipos de ambientes que se detallan a continuación para ser considerados al momento de sectorizar las áreas de estudio.

<u>AREAS VERDES</u>, en el Planner se las identifica con color verde y su perímetro de negro, debido a que no refleja ni refracta la luz, aunque pueda obstruir la línea de vista de un enlace de tránsito, tal como se muestra en la Figura 4-10.

Figura 4-10 Áreas Verdes de la FIEC

<u>BLOQUES DE AULAS</u>, los cuales se consideran como ambiente indoor recargado, tienen ventanas, colocando las zonas de color rojo y el borde de color azul en el planner. En la siguiente figura se muestra un bloque de aulas de la FIEC:

Figura 4-11 Bloques de Aulas de la FIEC

ZONAS DE DISTRACCIÓN, se las considera como áreas outdoor sin borde, en el simulador se definen de color gris y el borde de negro ya que no bloquea la señal de cobertura. En la Figura 4-12 se presenta una zona típica para este tipo de área dentro de la Facultad.

Figura 4-12 Área de distracción y estudio de la FIEC

En la Figura 4-13 se muestra la parte central de la FIEC en donde se destacan varios ambientes a diferentes alturas, lo cual hay que considerar al momento de sectorizar las zonas en el simulador.

Figura 4-13 Área Central de la FIEC

Otro ambiente a destacar es el que presenta el edificio central o también conocido como el Edificio Inteligente de la FIEC, donde se encuentran oficinas administrativas, laboratorios, aulas y Auditorio. Este bloque se lo debe considerar como un ambiente indoor abierto pero sin paredes, por lo que en el Planner se debería definir la zona de color azul y el perímetro gris.

Figura 4-14 Edificio Central de la FIEC

Una vez identificados cada unos de los ambientes con sus respectivos límites o perímetros en la FIEC, se debe proceder a ubicar los diferentes ambientes en la imagen importada al Planner.

A continuación se muestra como quedaría la imagen sectorizada en el Planner Simulator:

Figura 4-15 Definición de Ambientes en el Área de la FIEC

Luego de haber sectorizado la imagen, en el simulador se debe colocar a cada área su respectiva altura tomadas de mediciones reales en el lugar de estudio. La siguiente figura muestra la ventana donde se ingresa el valor en metros:

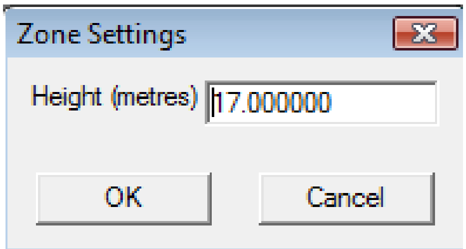


Figura 4-16 Indicador de altura para la creación de Zonas

A continuación se muestra la Tabla XXIX que indica la altura de cada una de las zonas creadas en el simulador (Figura 4-17):

Tabla XXXI: Tabla de alturas para las diferentes zonas de la FIEC

Area	Identificativo	Altura [m]
Edificio	1	7
Edificio	2	8
Edificio	3	10
Edificio	4	13.5
Edificio	5	15.5
Laboratorios de Computación	6	5
Aulas de Computación	7	9
Laboratorios Automatización	8	6
Laboratorios Electrónica/ Digitales	9	10
Laboratorio Redes Eléctricas	10	7
Laboratorio de Potencia	11	6
Antiguo Sala de Profesores	12	10
SASE	13	10
Comedor	14	10
Aulas FIEC	15	17.5
Piso Patio Central Bajo	16	5
Piso Patio Central Alto	17	6.5
Zona de Distracción	18	13.5
Areas Verdes	19	9
Areas Verdes	20	7
Areas Verdes	21	9
Areas Verdes	22	10
Areas Verdes	23	12
Areas Verdes	24	13
Areas Verdes	25	15
Areas Verdes	26	17
Parqueaderos	27	0

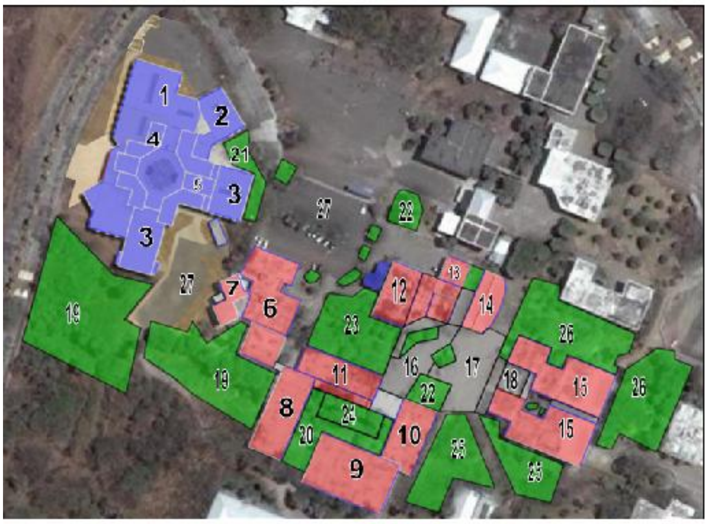


Figura 4-17 Identificación de Zonas en la FIEC

4.6 UBICACIÓN DE LOS PUNTOS DE ACCESO

En el diseño teórico planteado como solución mesh para la FIEC se tiene 5 APs y un AP@NAP. A continuación se muestra los APs en el simulador.

Figura 4-18 Ubicación de APs en el simular

A continuación se muestra el resultado de la cobertura simulada:

Figura 4-19 Cobertura simulada

Donde se puede concluir que con el diseño planteado teóricamente se logra cubrir gran parte del área de la FIEC pero no el 100%, por lo cual se plantea colocar varios APs más a la red para mejorar el área de cobertura, aumentar la redundancia y mejorar las tasas de transmisión de datos.

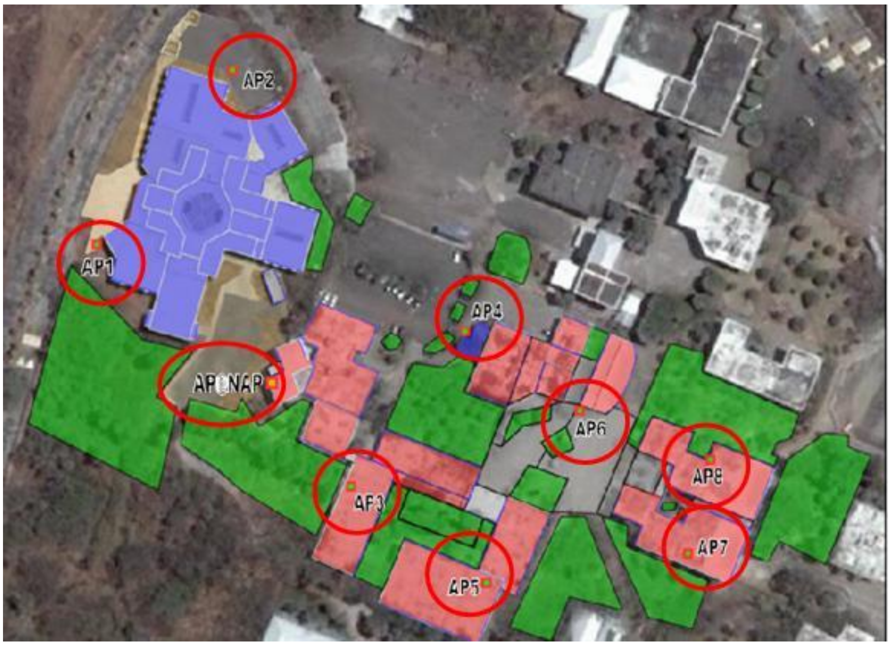


Figura 4-20 Ubicación de los nuevos puntos de acceso en la FIEC

Cabe recalcar que al ingresar un punto de acceso en el planner, éste nos muestra una ventana donde se ingresan los datos principales de una antena, como son el tipo de antena para el enlace de acceso, la altura del equipo, el nombre otorgado y la dirección MAC para que sea identificada dentro de la red Mesh. La Figura 4-21 muestra la ventana mencionada donde se debe ingresar los datos para cada punto de acceso:

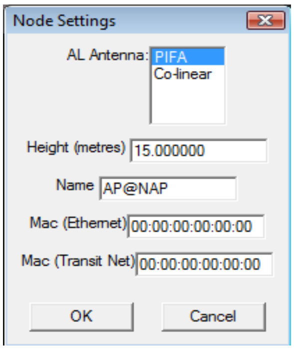


Figura 4-21 Indicador de altura para la creación de Puntos de Acceso

El proceso mencionado de ingresar datos se lo realiza para cada AP incluido el punto AP@NAP. La Tabla XXX muestra la altura que se le otorgó a cada equipo antes de obtener la cobertura simulada.

Tabla XXXII: Tabla de alturas para los diferentes Puntos de Acceso de la FIEC

Punto de Acceso	Altura [m]
AP@NAP	15
AP1	11
AP2	11
AP3	12
AP4	15
AP5	18
AP6	15
AP7	23
AP8	21

Los puntos de acceso que se utilizan para el estudio y planificación de la red Mesh emplean antenas de tipo PIFA para la cobertura del enlace de acceso. El uso de este tipo de antena presenta algunas ventajas importantes como la facilidad de acceso de un usuario incluso si está dentro de un ambiente y el punto de acceso está en el exterior. Otra ventaja es que utiliza la polarización tanto vertical como horizontal de manera conjunta para aumentar la ganancia y por ende mejorar el rendimiento.

4.7 CONECTIVIDAD ENTRE LOS PUNTOS DE ACCESO

Como se ha mencionado en capítulos anteriores el enlace de tránsito permite la conectividad de los puntos de acceso, por tal razón la ubicación y la altura a la cual se ubicará los APs es importante puesto que deben permitir que exista línea de vista LOS entre cada uno de ellos.

La FIEC presenta varias edificaciones y áreas verdes de gran altura, que producen reflexión y refracción del enlace dependiendo del grado de atenuación de la edificación que se encuentre obstaculizando. Por esta razón se debe asegurar al menos un enlace de Tránsito para cada punto de acceso para que exista comunicación de los equipos y tener una topología acorde a los requerimientos y necesidades que se presenten en los usuarios.

A continuación se muestra el plano de la FIEC con los puntos de acceso ubicados y sus respectivos enlaces de Tránsito, que son identificados por diferentes colores que indican la tasa máxima de transmisión expresada en Mbps que tiene cada enlace (Figura 2-23):

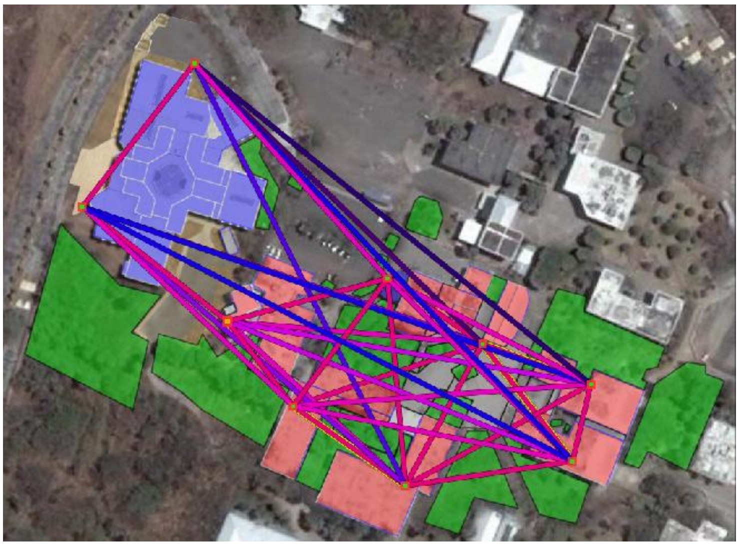


Figura 4-22 Enlaces de Tránsito de los Puntos de Acceso en la FIEC

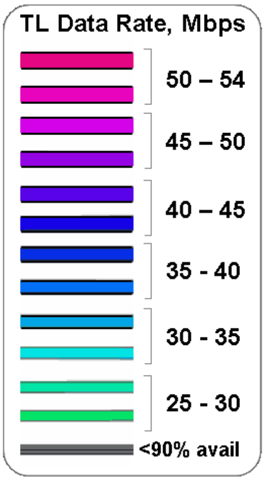


Figura 4-23 Colores que identifican la tasa de transmisión de los enlaces de tránsito

De acuerdo a los resultados obtenidos podemos indicar que los enlaces que están de color Fucsia aseguran una tasa de datos mayor de 50 Mbps, mientras que los enlaces de color Violeta aseguran una tasa de datos de 45 a 50 Mbps, y los enlaces de color Azul son enlaces con tasa de datos de 40 a 45 Mbps. No se observan enlaces de otro color que son identificados de enlaces de poca tasa de transmisión como pueden ser de color Celeste o de color Verde.

En base a los enlaces de tránsito con tasa de datos de 54Mbps, podemos realizar una topología que asegura un modelo de red Mesh de excelente rendimiento, el cual garantiza enlaces redundantes en caso de que algún punto de acceso quede fuera de servicio por algún motivo. A continuación se presenta una topología en base a los datos de simulación obtenidos en el Planner:

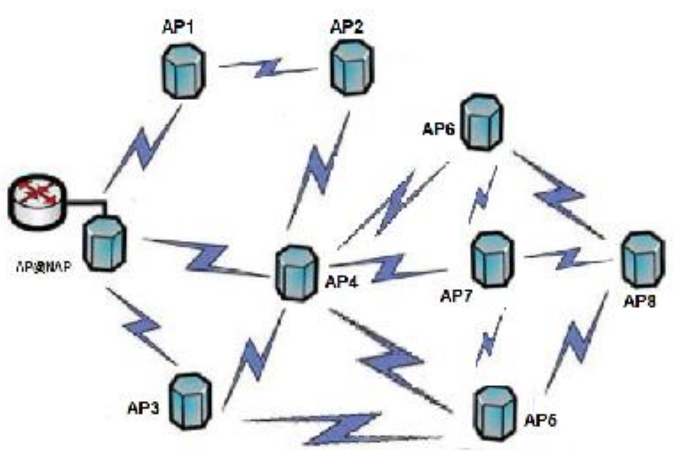


Figura 4-24 Topología de Red basados en resultados simulados en el Planner

4.8 MAPA DE COBERTURA

El enlace de acceso como se ha mencionado permite la conectividad de los APs con los usuarios, por tal razón la buena ubicación y la altura indicada de éstos permite que exista un área de mayor cobertura para la facilidad de conexión de los usuarios finales hacia la red Mesh.

Al realizar las pruebas de simulación, el análisis de propagación no es idéntico a los datos teóricos como se ha mencionado, esto se debe a la gran cantidad de áreas verdes y al terreno irregular que se presenta en la Facultad donde tenemos diferentes niveles de piso, para lo cual tomamos como referencia el parqueadero como nivel 0. Adicional factores de atenuación de cada uno de los ambientes, como son las aulas, laboratorios, edificio central afectan el modelo ideal de propagación.

En la Figura 4-25 se muestra los colores que resultarían en una simulación en el Planner de acuerdo a la tasa de transmisión.

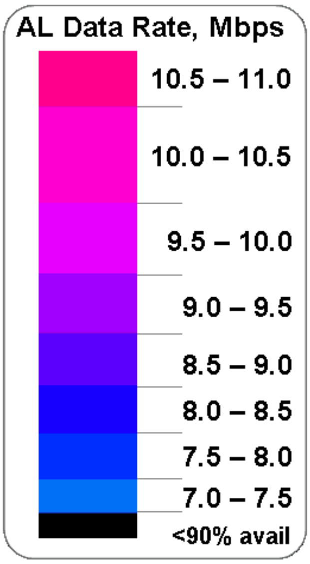


Figura 4-25 Colores que identifican la tasa de transmisión de los Enlaces de Acceso

A continuación se presenta los resultados que se obtuvieron al generan el área de cobertura del enlace de Acceso con los APs que se añadieron:

Figura 4-26 Resultado de Simulación del Enlace de Acceso con los APs añadidos

Nótese que la mayor parte de la geografía esta de color Fucsia lo que nos indica que más del 90 % tiene asegurada una tasa de transmisión de 54Mbps, salvo el caso de las áreas verdes que se encuentran cercanas a la ubicación del punto AP@NAP, que debido a factores de atenuación no se propaga la señal, pero que no afectaría el servicio ya que es un lugar donde no hay presencia de usuarios. Otra área en la cual no se observa cobertura está en la parte superior central de la Figura 4-26, la cual no pertenece al área de la FIEC y por tal razón no es parte del análisis de cobertura del enlace.

Como se apreció la cobertura mejoró considerablemente aumentándole varios APs al diseño planteado teóricamente, por las razones ya detalladas.

4.9 SOLUCIÓN EN 3D

El Planner tiene dos opciones para mostrar los resultados la ***vista plano*** la cual se ha mostrado en figuras anteriores y la ***vista perspectiva*** que muestra los resultados en 3D.

En la vista perspectiva se puede observar la diferencias de alturas entre ambientes y APs, lo cual es importante para la implementación de la solución mesh ya que nos muestra si existe línea de vista LOS entre los nodos.

Además la vista en 3D en el simulador permite verificar si se puede lograr un enlace de tránsito óptimo entre nodos, considerando evitar que áreas verdes o edificaciones obstaculicen la línea de vista, para lo cual los puntos de acceso deben tener una altura ideal pero que se encuentre dentro de los parámetros permitidos, así como asegurar que todos los puntos de acceso estén promediando el mismo nivel de altura y de esta manera evitar el uso de antenas auxiliares.

A continuación se muestra dos vistas perspectivas de la solución planteada para la FIEC, las cuales corroboran que la información ingresada está correcta y favorece a la obtención de resultados del enlace de Tránsito y enlace de Acceso ideales:

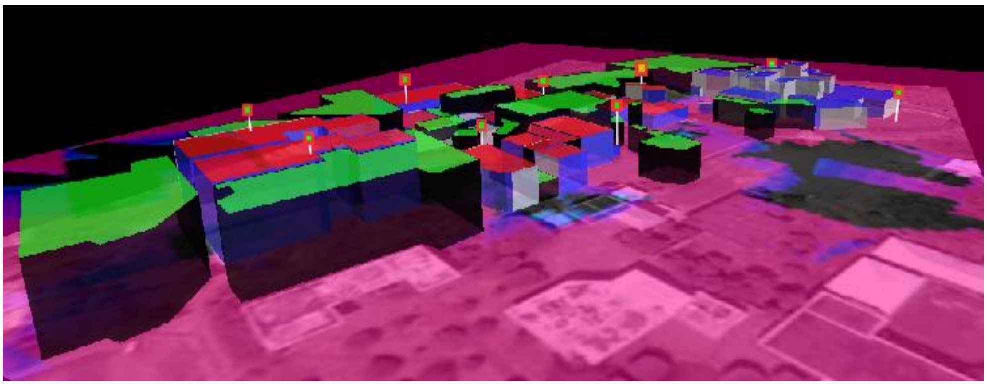


Figura 4-27 Vista Perspectiva de la FIEC utilizando el Planner

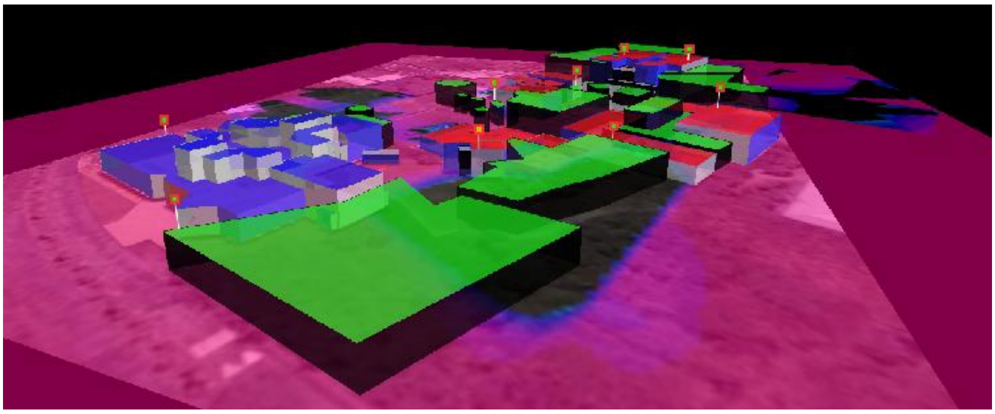


Figura 4-28 Vista Perspectiva de la FIEC de otro ángulo utilizando el Planner

4.10 HERRAMIENTA DE RF PARA MOSTRAR LA VELOCIDAD DE SERVICIO

Planner es una herramienta de diseño rápido de alto rendimiento para las redes inalámbricas Mesh.

El objetivo de aplicar en el estudio de la red el uso del software es para asegurar el máximo rendimiento independiente de las aplicaciones que utilizarán los equipos y los usuarios móviles de la red.

Esta completa herramienta permite diseñar redes inalámbricas que satisfagan usos específicos, requisitos de confiabilidad y rendimiento de su entorno.

La función de anticipar y visualizar el impacto de los puntos de acceso con respecto a los obstáculos como edificaciones y áreas verdes, interferencia en un canal común permiten que el diseño constituya un paso fundamental para brindar un rendimiento inalámbrico superior con la mejor calidad de servicio minimizando costos de instalación y mantenimiento.

El software de diseño RF es una herramienta basada en una aplicación para planificación del sitio, así como detectar y prevenir problemas.

Los mapas de RF muestran una ubicación óptima del punto de acceso, mientras que los gráficos de indicadores de cobertura representan el estado de la red indicando el alcance máximo que tiene cada punto de acceso mostrando la velocidad de servicio que se asegura para el uso de un nodo móvil, ya que al ser una cobertura Wifi para los usuarios se asegura un rendimiento máximo de 11 Mbps representada con colores que van de rojo a celeste que indica áreas de poco ancho de banda asegurado.

A continuación se presentan los gráficos de indicadores de cobertura que presenta el Planner:

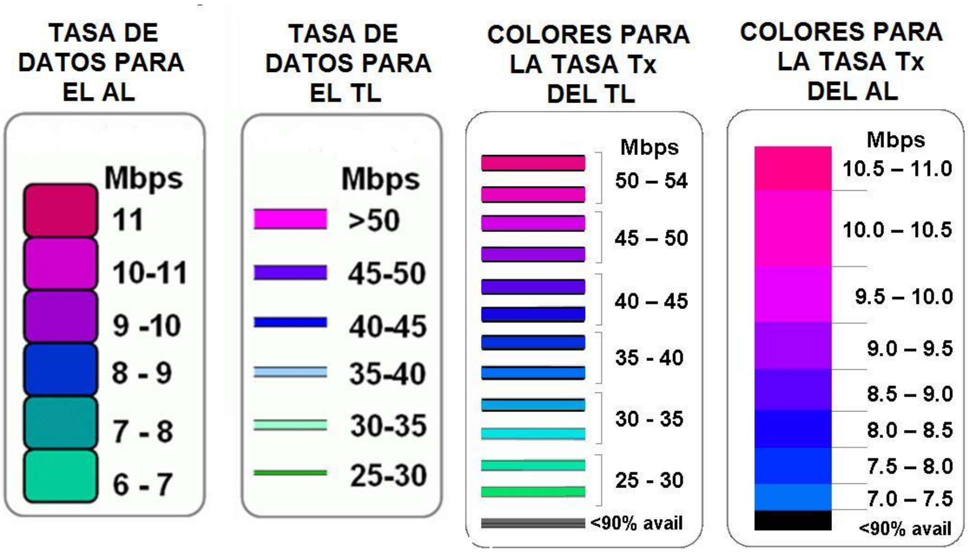


Figura 4-29 Indicadores de Cobertura

Los usuarios pueden verificar el estado y ubicación de los dispositivos de la infraestructura inalámbrica, detectar y solucionar problemas, generar informes y procesar datos. Estadísticas tales como cobertura de RF, balanceo de carga, redundancia y utilización de la red, se muestran gráficamente, permitiendo que los especialistas en tecnología informática evalúen el estado de la red.

4.11 COMPARACIÓN DE DATOS SIMULADOS Y TEÓRICOS

El diseño que se planteó como solución mesh para la FIEC consta de 5 AP7220 y un AP@NAP (Figura 4-30), luego de la simulación del diseño mencionado (Figura 4-31) se concluyó que no cumplía con el objetivo que era cubrir totalmente el área de la facultad, por este motivo se decidió aumentar el número de AP7220 (Figura 4-31), logrando cubrir el 100% del área de estudio (Figura 4-31).

Figura 4-30 Comparación de ubicación de puntos de acceso entre el diseño teórico y el diseño mejorado

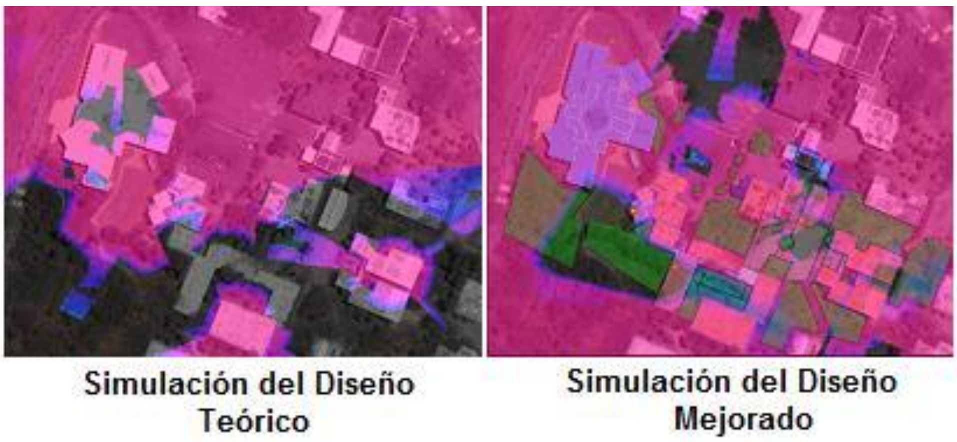


Figura 4-31 Comparación del área de cobertura entre el diseño teórico y el diseño mejorado

Cabe recalcar que en el diseño mejorado existe señal con poca intensidad en una parte de zona verde (Figura 4-32), lo cual es despreciable puesto que es una sector donde no hay demanda de servicio de la red.

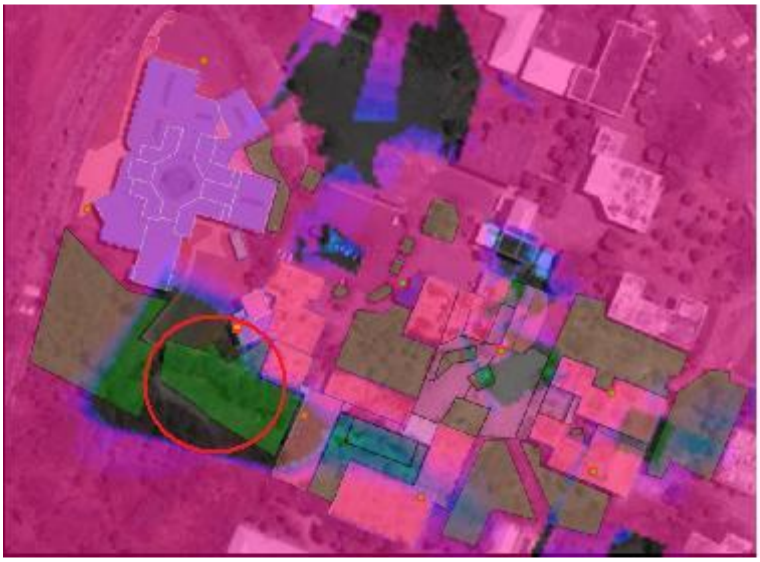


Figura 4-32 Detección de Zonas Muertas en el Diseño Mejorado

Entre la cobertura esperada teóricamente y la simulada la diferencia es que al simular se observa atenuación de señal en el sector del área verde ubicada cerca de los laboratorios de electrónica de la FIEC y alrededor del bloque de aulas (Figura 4-33), por esta razón como se mencionó se decidió aumentar el número de APs y la cobertura de la red mejoró, es decir la diferencia fue de 3 APs.

Figura 4-33 Detección de Zonas Muertas en el Diseño Teórico

CAPITULO 5

5. DESARROLLO DE UN PROTOTIPO DE UNA RED MESH PARA LA FIEC

5.1 ESQUEMA GENERAL DEL PROTOTIPO A DESARROLLAR

El prototipo que se desarrollara no tiene equipos de backup, pero servirá para demostrar cómo trabaja un nodo de la red mesh, para lo cual es necesaria una correcta implementación de las direcciones de red y configuración de los protocolos de enrutamiento y rutas.

Para la implementación del prototipo se debe tener en consideración una serie de parámetros que van a diferenciar nuestro modelo de diseño. El punto más destacado es que no se utiliza el router NAP, debido a que la red mesh solo se formará de los APs 7220 y 7215, para lo cual el equipo Wireless Gateway 7250 debe ser configurado para que soporte el AP 7220 como equipo AP@NAP.

Para el buen desempeño del prototipo es necesario tener en cuenta algunos puntos, los cuales deben ser considerados para la implementación de los equipos a utilizar:

- Conectar el punto de acceso AP 7220 con el equipo Gateway 7250 con un cable cruzado.
- Añadir una ruta por defecto en el Gateway 7250 para poder tener comunicación con el punto de acceso.
- En el punto de acceso AP 7220 debe estar configurado la puerta de enlace **GW** y el parámetro **Pktgw** apuntando a la dirección IP del equipo Wireless Gateway 7250.
- En el servidor NOSS se debe configurar los archivos **ap.ftp** y **dhcpd.conf** para que apunten a la dirección IP de la interface del equipo Gateway 7250 que se conecta al punto de acceso, y además registrar los puntos de acceso a utilizarse.
- Utilizar un router de borde hacia el Internet para que permita realizar un NAT, preferible de manera dinámica para que los usuarios móviles una vez que son autenticados tengan la facilidad de conexión hacia el Internet de manera automática

utilizando el servidor DHCP que es el encargado de asignar la dirección IP a los usuarios.

- Utilizar un switch de capa 2 para conectar la interface publica del equipo Gateway 7250, el servidor NOSS y el router de borde que permite la salida hacia el Internet.

A continuación se presenta el esquema del prototipo que se implementó en la facultad de la FIEC, mostrando de manera gráfica la topología de red y direcciones de red que se utilizó en los equipos:

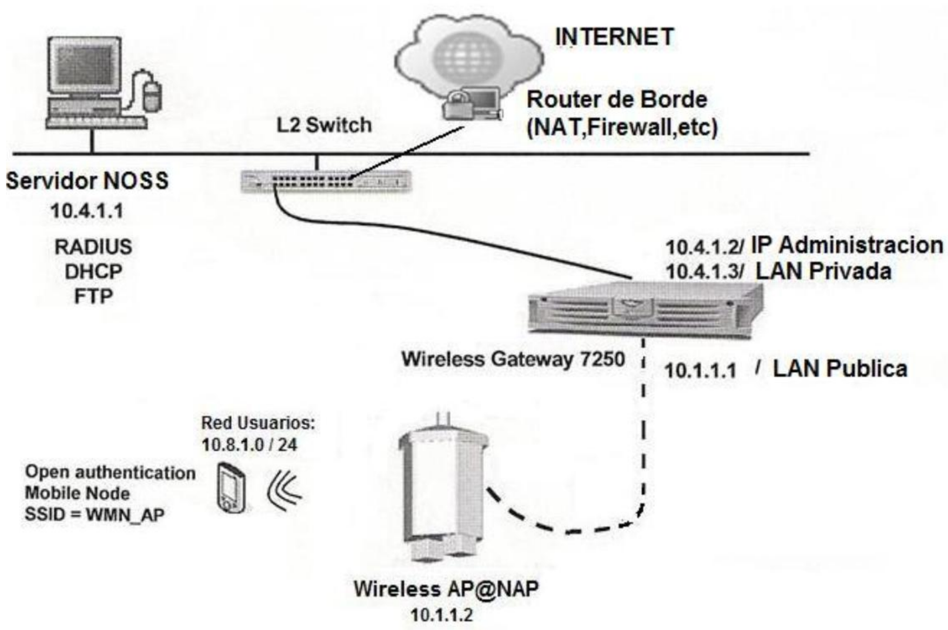


Figura 5-1 Diagrama del Prototipo de la red Mesh en la FIEC

5.2 DIRECCIONAMIENTO IP

De acuerdo a las características que se indicaron en el punto anterior, se han asignado las siguientes direcciones IP para los equipos que forman parte de la infraestructura Mesh:

Tabla XXXIII: Direccionamiento IP para el prototipo de la red Mesh

ELEMENTO	DIRECCIONAMIENTO IP
Servidor NOSSwin Radius, DHCP y FTP Server:	10.4.1.1 / 24
Wireless Gateway 7250 IP de Administración: IP Privada: IP Publica:	 10.4.1.2 / 24 10.4.1.3 / 24 10.1.1.1 / 24
AP@NAP:	10.1.1.2 / 24
Usuarios Terminales:	10.8.1.x / 24

Como se muestra en la tabla XXXIII las direcciones utilizadas pertenecen a redes privadas, ya que es un despliegue de equipos en una red LAN. Para que los usuarios puedan navegar hacia el Internet, tanto el servidor NOSS como el equipo Wireless Gateway 7250 enrutan las redes privadas hasta un router de borde que puede ser proporcionado por el proveedor de servicio de Internet o configurado por el desarrollador de la red Mesh, el cual debe tener configurado un NAT para permitir las peticiones de los usuarios hacia el Internet, facilitando la navegación y transmisión de datos.

Adicional el protocolo de enrutamiento que se emplea en los equipos de Nortel es OSPF, el cual es configurado en el equipo Wireless Gateway 7250 donde la ruta por defecto es **10.0.0.0**

5.3 CONFIGURACIÓN DE LOS ELEMENTOS DE LA RED MESH

5.3.1 NOSS

El servidor NOSS se lo puede instalar en cualquier computadora, para lo cual se debe hacer doble clic en el instalador **NOSSwin_v098b6b.exe**, donde se observará la siguiente imagen:

Figura 5-2 Aplicación del Servidor NOSS

El servidor necesita crear una partición interna, para lo cual solicita la creación de una unidad S:

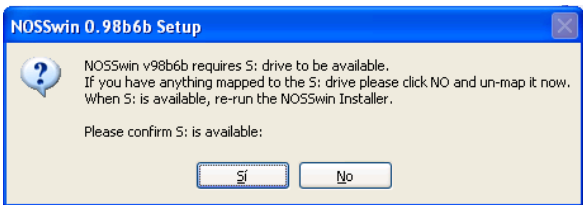


Figura 5-3 Creación de unidad adicional en el servidor NOSS

Se presenta una ventana donde empieza la instalación, en la cual se hace clic en **Next:**

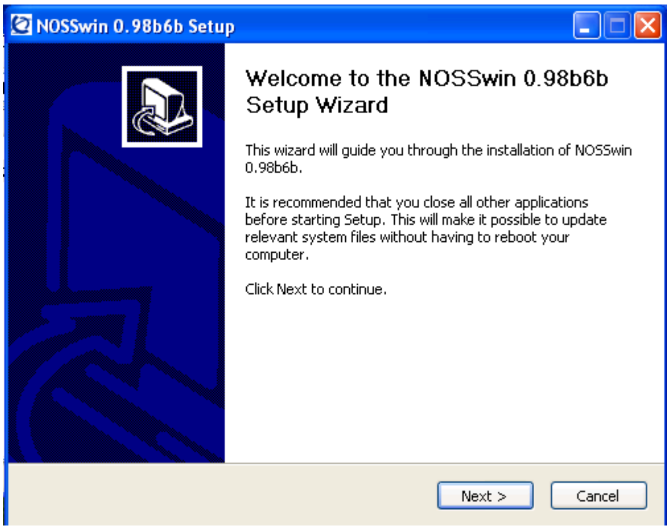


Figura 5-4 Instalación del servidor NOSS

A continuación se escoge los componentes como el servicio del Radius, FTP, DHCP y SNMP que es encargado del monitoreo, los mismos que están señalados en la siguiente figura:

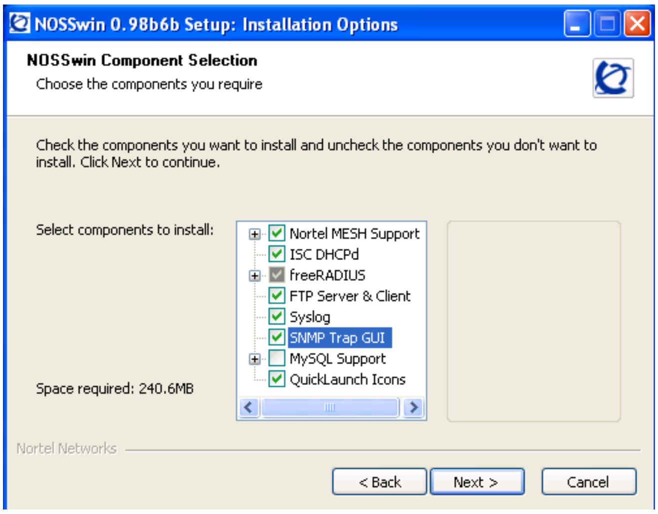


Figura 5-5 Instalación de Compentes del servidor NOSS

Durante la instalación, se debe escoger el firmware que soportará el servidor NOSS, para el caso de estudio se escogerá la versión 3.x, que permitirá realizar actualizaciones mediante FTP para el punto de acceso AP y verificación de los usuarios mediante el archivo de control:

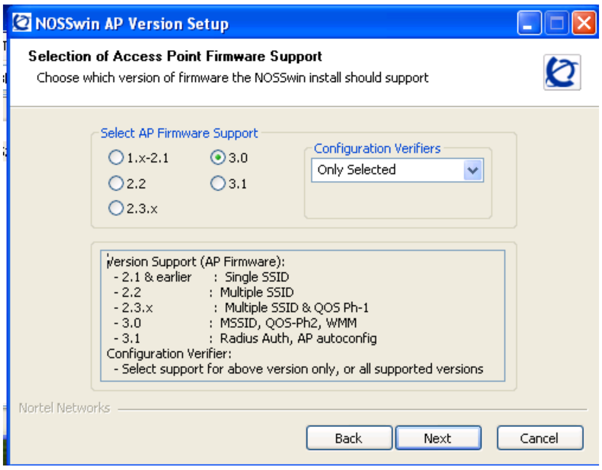


Figura 5-6 Selección del Firmware para el servidor NOSS

Una vez seguidos estos pasos queda instalado el servidor NOSS para poder correr sus aplicaciones:

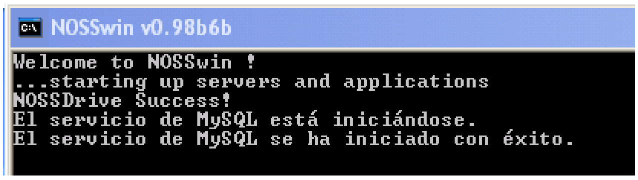


Figura 5-7 Inicio del servidor NOSS

5.3.1.1 SERVIDOR RADIUS

Los archivos de configuración del servidor Radius se encuentran en la dirección:

C:\NOSS\Servers\Radius\config

El archivo ejecutable del servidor es identificado como **radiusd.exe**. Para inicializar el **freeRadius** debe inicializarse tal como muestra la figura 5-8:

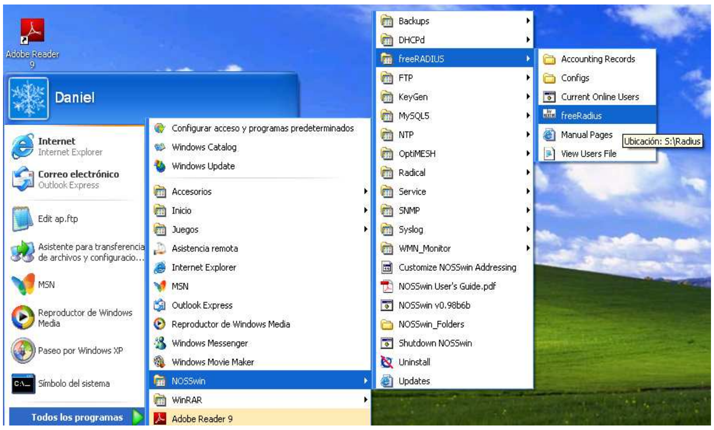


Figura 5-8 Inicialización del freeRadius

La figura 5-9 muestra los archivos de configuración de la herramienta **Keygen**, que permite configurar y modificar los archivos del servidor:

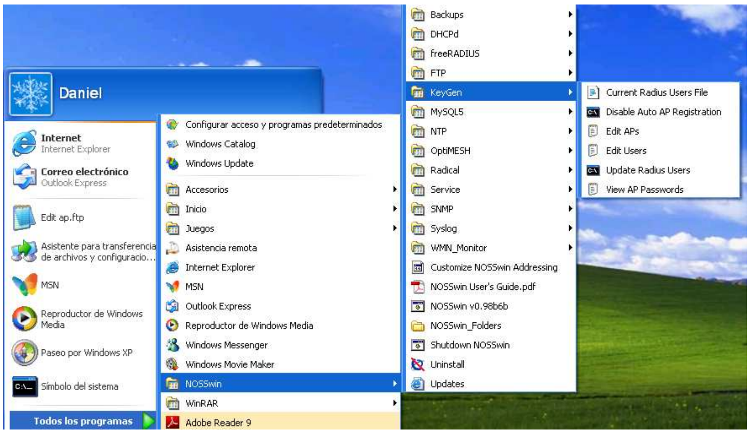


Figura 5-9 Utilizacion de la herramienta Keygen para el Servidor Radius

CONFIGURACION DE LOS ARCHIVOS DE CONFIGURACIÓN DE LA HERRAMIENTA KEYGEN

PRIMERO

Se modifica el archivo **in.txt** para editar los números de serie de los puntos de acceso AP instalados. Siempre el punto AP@NAP debe estar al inicio de la lista del archivo. La ruta del archivo a configurar es la siguiente:

Inicio -> Programas -> NOSSwin -> Keygen -> Edit APs

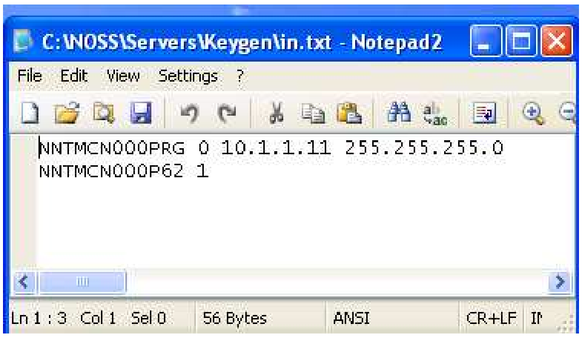


Figura 5-10 Registro de los puntos de acceso AP para el servidor NOSS

SEGUNDO

Se edita el archivo **users.txt.** Si el tipo de protocolo de seguridad utilizado es WPA, entonces se crea un usuario EAP por defecto con clave ‘secure’. La ruta del archivo a configurar es la siguiente:

Inicio -> Programas -> NOSSwin -> Keygen -> Edit Users

En el archivo de usuarios debe constar lo siguiente:

- Nombre del equipo, por lo general se ingresa la dirección MAC.
- Tipo de autenticación que en este caso es EAP.
- Contraseña para el equipo.
- SSID para la conexión de los equipos.
- Tunnel ID, para brindar seguridad al enlace.

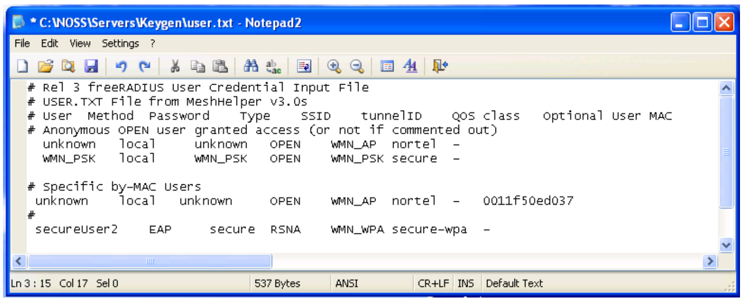


Figura 5-11 Registro de las cuentas SSID para el servidor NOSS

TERCERO

Se debe generar el archivo **out.txt**, para lo cual se selecciona la siguiente ruta:

Inicio -> Programas -> NOSSwin -> Keygen -> Update Radius Users

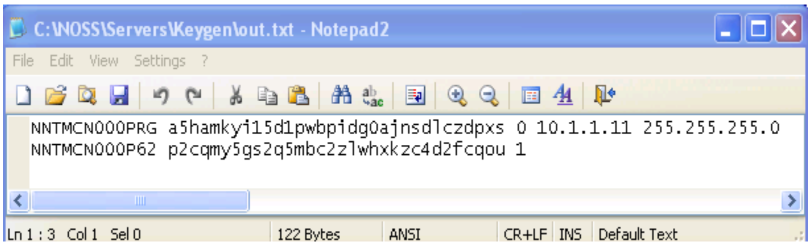


Figura 5-12 Generacion de Passwords de los puntos de acceso AP en el servidor NOSS

5.3.1.2 SERVIDOR DHCP

Para inicializar la aplicación del servidor DHCP se debe seleccionar el ejecutable **ISC DHCPd** tal como se muestra la siguiente figura:

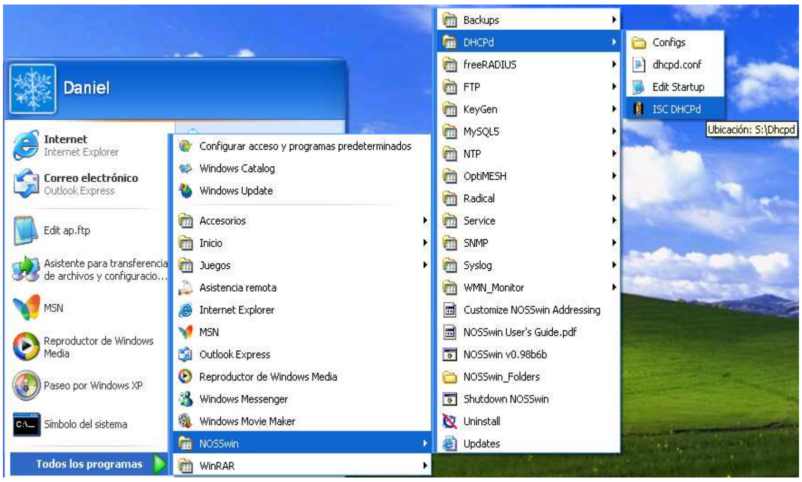


Figura 5-13 Inicialización del Servidor DHCP

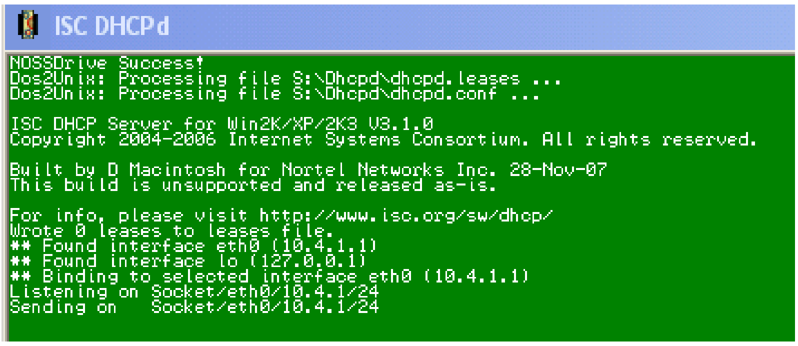


Figura 5-14 Aplicación ISC DHCPd

Para que el servidor DHCP pueda funcionar de manera correcta de acuerdo a los equipos instalados y a las necesidades de la red, se debe modificar el archivo **dhcpd.conf,** tal como se encuentra el archivo de configuración en el ANEXO G.

5.3.1.3 SERVIDOR FTP

El servidor FTP se encuentra preconfigurado y preinstalado al momento de trabajar con la red Mesh. Este servidor inicia sesión como un servicio de respaldo cada vez que el NOSSwin arranca, así no se encuentren usuarios conectados. Para iniciar una sesión FTP se debe iniciar el FTP Server Monitor, tal como se observa en la figura 5-15:

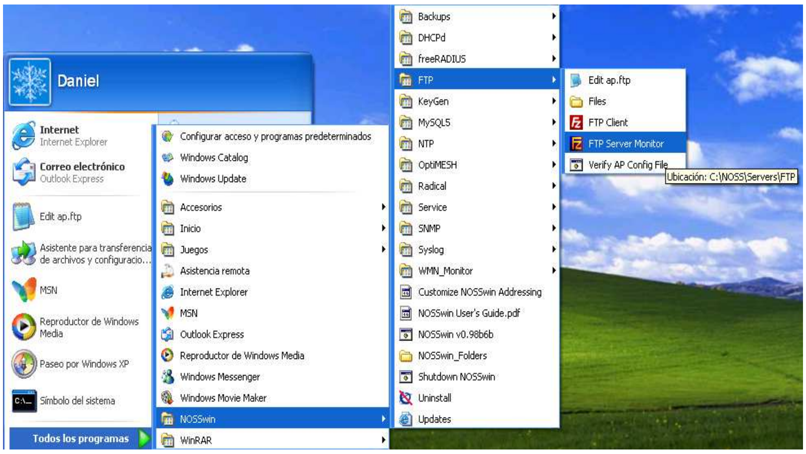


Figura 5-15 Inicialización del Servidor FTP

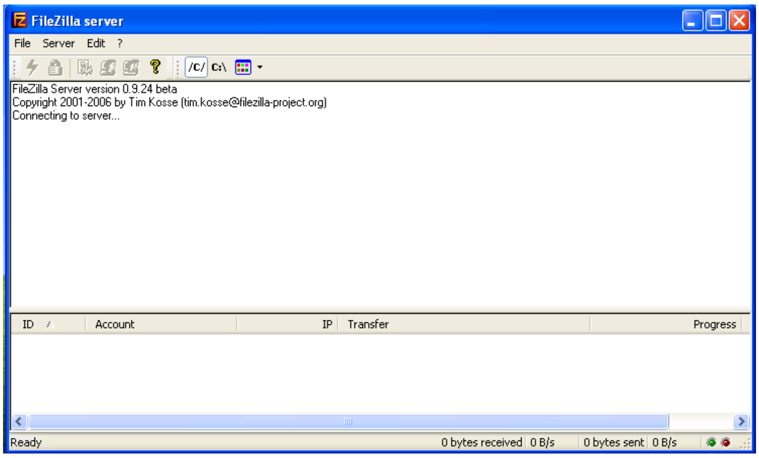


Figura 5-16 Aplicación del Servidor FTP: FileZilla Server

5.3.2 WIRELESS GATEWAY 7250

Para configurar las interfaces del Wireless Gateway 7250, administrativa y privada, es necesario hacerlo a través de una sesión HyperTerminal.

En el menú principal, se selecciona la interface de administración y se coloca la dirección IP que se definió en el diseño: **10.4.1.2**.

La segunda dirección IP es privada puesto que es la interface de la LAN, para lo cual se ingresa la dirección: **10.4.1.3**, con máscara de red **255.255.255.0.**

Una vez configuradas las IPs se puede ingresar al equipo mediante Web browser colocando la dirección IP de administración, tal como se muestra en la siguiente figura:

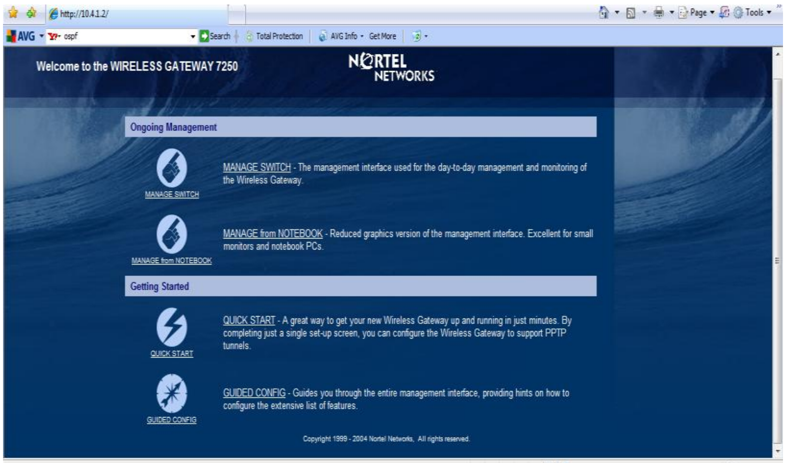


Figura 5-17 Wireless Gateway 7250 Web Client

Para iniciar la configuración de la interface pública, rutas por defecto y habilitación de servicios se ingresa a **MANAGE SWITCH.**

SERVICIOS DE ADMINISTRACIÓN

Para habilitar los servicios de FTP, Telnet y SNMP, se selecciona **SERVICES> AVAILABLE** y en la opción de

Management Protocol se selecciona **HTTP**, **SNMP**, **FTP** y **Telnet**, tal como se muestra en la figura 5-18:

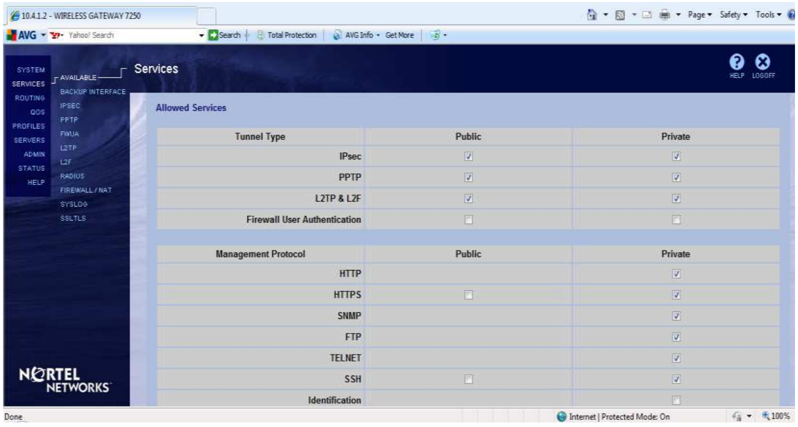


Figura 5-18 Habilitación de Servicios de Administración en el Gateway 7250

CONFIGURACIÓN DE LA INTERFACE LAN PÚBLICA

Para configurar la dirección IP se hace clic en **SYSTEM> LAN.** Se edita la IP de la interface Fast Ethernet 2 con la 10.1.1.1 como se muestra en la figura 5-19.

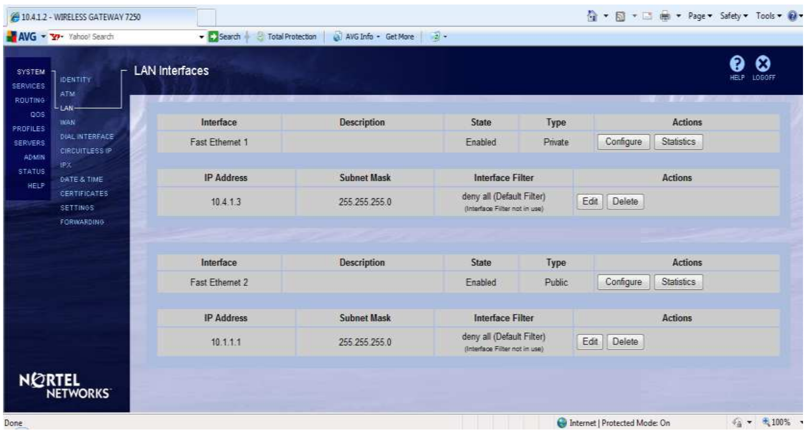


Figura 5-19 Configuración de la Interface LAN Pública

CONFIGURACIÓN DE RUTAS POR DEFECTO

Para poder establecer la comunicación entre el Wireless Gateway 7250 y el punto AP@NAP así como del Gateway 7250 hacia el servidor NOSS y el router de borde, es necesario añadir rutas por defecto.

Se hace clic en **ROUTING> STATIC ROUTES**, se escoge la opción **Add Public Route** y se coloca la dirección IP **10.1.1.1**. En la opción **Add Private Route** se coloca la IP privada que hace de puerta de enlace en el router de borde **10.4.1.10.**

Adicional se debe asegurar en ambos casos que el campo **Admin State** se encuentre en **enable** y el costo sea de **10**. A continuación se muestra la ventana donde se configura las rutas:

Figura 5-20 Configuración de Rutas Estáticas en el Gateway 7250

CONFIGURACIÓN DEL FIREWALL

El Firewall tiene como objetivo crear las respectivas políticas y filtros para administrar el flujo del tráfico, así como también configurar el enrutamiento global.

HABILITACIÓN DEL STATEFUL FIREWALL:

Se selecciona **SERVICES> Firewall** / **NAT**, y en la ventana se selecciona **Firewall>Stateful Firewall**. Al final de la ventana se debe deshabilitar la opción **Tunnel Filter.**

CREACIÓN DE LA POLÍTICA Y FILTROS:

Se selecciona **SERVICES> Firewall** / **NAT**, y en la ventana se selecciona **Manage Policies** en la columna de **Action.** Luego aparece una nueva ventana donde se crea la política, tal como se observa en la siguiente figura:

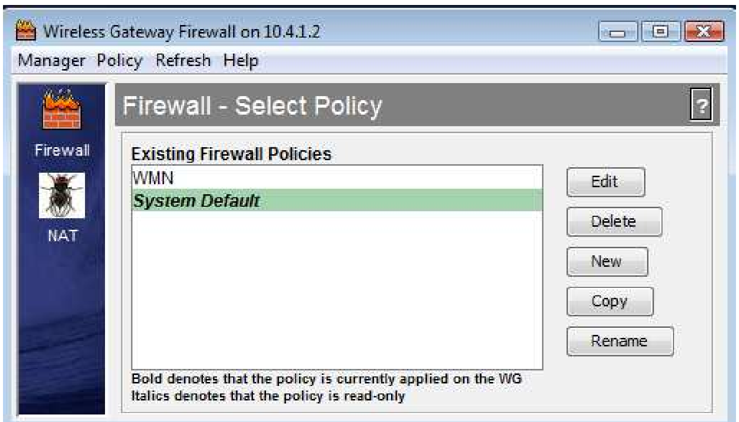


Figura 5-21 Creación de una Política en el Firewall del Gateway 7250

Para este caso es necesario crear tres diferentes tipos de filtro que cumplirán con la siguiente función:

- El primer filtro permitirá que el tráfico de señalización móvil IP alcance al agente de base (home agent) en el Wireless Gateway.

- El segundo filtro permitirá que el tráfico desde la red privada LAN pase a través del Wireless Gateway 7250 a la red pública LAN.

- El tercer filtro permite que el tráfico dentro de un túnel IPsec logre llegar a cualquier destino, tanto en la LAN privada como en la LAN pública.

Los filtros creados en la política se pueden observar en la siguiente ventana:

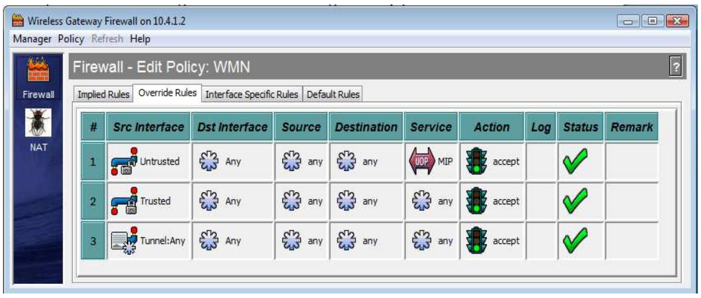


Figura 5-22 Creación de Filtros en una Política del Gateway 7250

En el caso del primer filtro es necesario crear un Objeto de Servicio, que habilite el puerto **434** y que permitirá el tráfico de señalización, tal como se muestra en la figura:

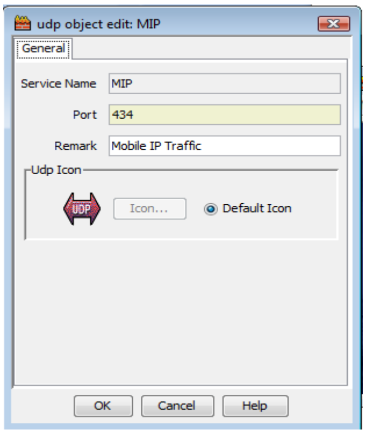


Figura 5-23 Creación de un Objeto de Servicio para aplicar Filtros

Finalmente, una vez creada la política con sus filtros respectivos se escoge la política en **Policy**, como se indica en la siguiente ventana:

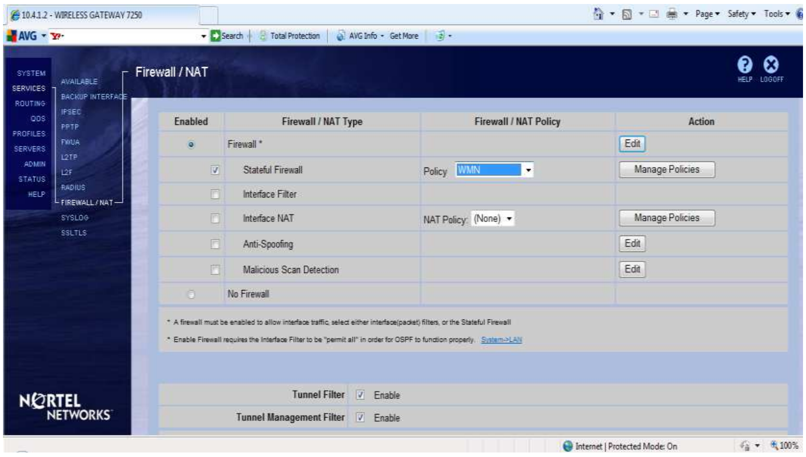


Figura 5-24 Selección de la Política aplicada al Firewall del Gateway 7250

CONFIGURACIÓN DE PUNTOS DE ACCESO AP 7220 EN EL GATEWAY 7250

Se necesita personalizar los perfiles de una cuenta de un punto de acceso para asegurar la seguridad en el túnel IP creado.

Para crear una cuenta se debe escoger la siguiente ruta: **PROFILES > USERS** y en el menú **Group** se selecciona **Base/AP/@NAP.**

Luego, se debe hacer clic en **Add User** donde aparece otra ventana que permite ingresar el nombre con el cual se va a identificar al punto de acceso.

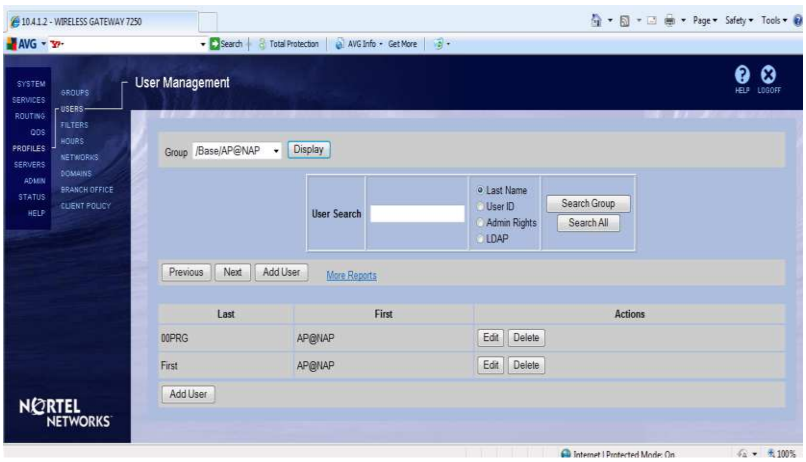


Figura 5-25 Configuración de Cuenta AP 7220 en el Wireless Gateway 7250

En otra ventana tenemos la opción de **User Accounts** y en la línea de **IPSec** se ingresa el número de serie del punto de acceso y el password del equipo que es el mismo que se obtuvo al ejecutar el archivo **output.txt** que forma parte del servidor NOSS. La siguiente figura muestra la opción a configurar:

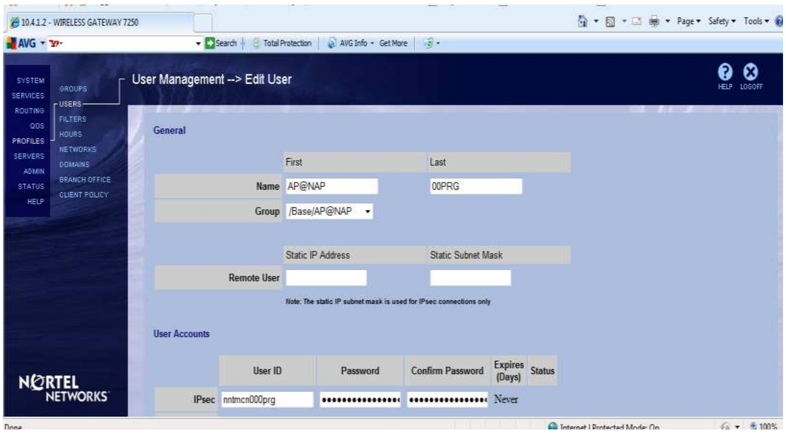


Figura 5-26 Configuración de Password de un punto AP 7220 en el Gateway 7250

Para configurar puntos de acceso adicionales y formar la red Mesh se sigue el mismo procedimiento, pero en la opción de **Group** se escoge el ícono de /**Base**/**Standalone** ya que serán puntos de acceso que permitirán tener los enlaces de tránsito para tener una cobertura mayor de la red.

5.3.3 WIRELESS AP 7220 Y AP 7215

A continuación se presenta los pasos para la configuración de los APs 7220 y 7215.

PRIMERO:

Para la configuración del punto de acceso AP@NAP es necesario configurar una serie de parámetros entre ellos la dirección IP estática:

WMN7220#configure

WMN7220(configure)#set role @nap (Se ingresa 'Yes' para aceptar el role)

WMN7220(configure)#set ip 10.1.1.11

WMN7220(configure)#set mask 255.255.255.0

SEGUNDO:

Se ingresa el área del OSPF, que es el protocolo de enrutamiento que se utiliza en la configuración de equipos:

WMN7220(configure)#set areaid 10.0.0.0

Luego se configura la dirección IP Pública del equipo Wireless Gateway y la dirección del Router por Defecto:

WMN7220(configure)#set pktgw 10.1.1.1

WMN7220(configure)#set gw 10.1.1.1

La Figura 5-27 muestra los parámetros configurados mediante el comando show:

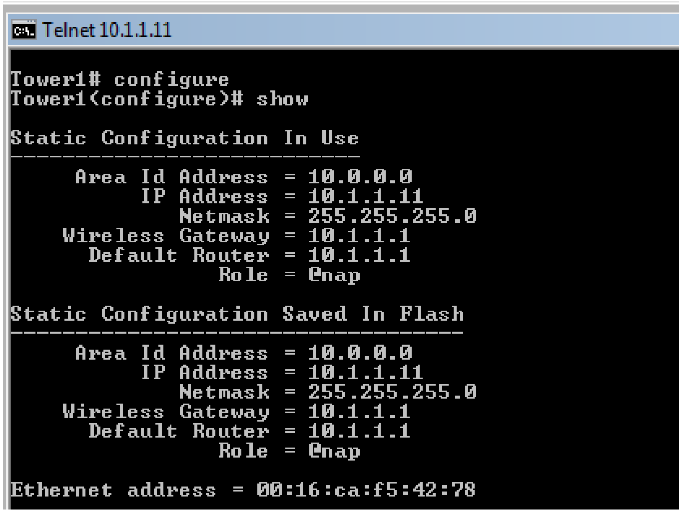


Figura 5-27 Configuración del punto de acceso AP@NAP

TERCERO:

Se configura la información para los parámetros de Administración:

WMN7220#configmgr

WMN7220(configmgr)#set server 10.4.1.1

WMN7220(configmgr)#set file ap.conf

WMN7220(configmgr)#set user NortelWarp

WMN7220(configmgr)#set passwd nortelWarp

La figura 5-28 muestra los parámetros configurados mediante el comando show:

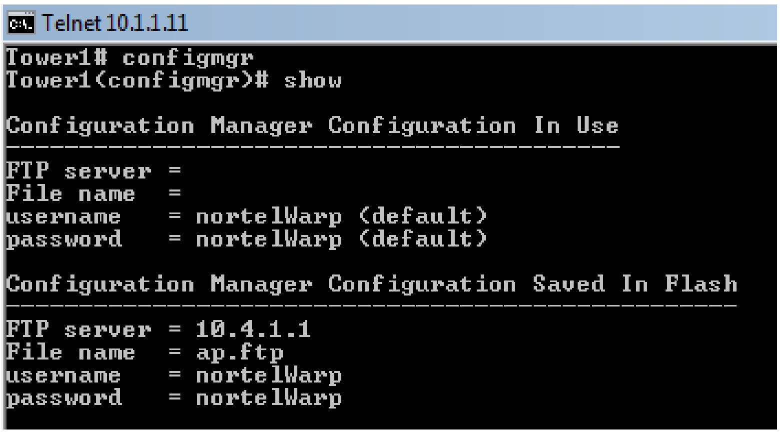


Figura 5-28 Configuración de Administración del punto de acceso AP@NAP

Es muy importante tener configurado de manera correcta el archivo ap.conf, en el cual se definen parámetros que se conocen como bloques, que se encargan de la identificación de redes, SSID, enlace de acceso AL, DHCP y demás detalles que se muestran en el ANEXO I.

5.3.4 ROUTER DE BORDE

Este equipo es el encargado de que los usuarios móviles puedan tener salida hacia el Internet, ya que recepta las direcciones IP privadas de la red Mesh y las traduce por medio de un NAT dinámico hacia las direcciones públicas que haya proporcionado el proveedor ISP.

Para el caso del router no es necesario que sea de la misma marca de los equipos de solución Mesh, ya que sólo es encargado de enrutar las redes. En este caso se utiliza el router modelo 1605 de la marca Cisco.

En lo que respecta a la configuración del router de borde, éste debe tener al menos dos interfaces Ethernet. En una interface se configura la red WAN, esta red la asigna el proveedor de internet ya que es la red pública. En la otra interface Ethernet se colocan dos redes privadas, la dirección 10.4.1.10/24 que pertenece a la red de administración del Gateway y el servidor NOSS, y la dirección 10.8.1.254/24 que pertenece a la red que el servidor DHCP asigna a los usuarios móviles.

En el ANEXO J se muestra una configuración más detallada del equipo mencionado.

5.4 VERIFICACIÓN DE AUTENTICACIÓN DE UN USUARIO

Un usuario móvil atraviesa por diferentes fases para completar la conectividad hacia la red:

El usuario móvil encuentra un punto de acceso AP o punto AP@NAP para asociarse con algún SSID de la red Mesh. En el prototipo desarrollado se ha implementado tres SSIDs: WMN_AP, WMN_PSK y WMN_WPA, es decir el primero sin seguridad y los dos siguientes con llave de seguridad. La siguiente figura muestra las alternativas que tiene un usuario para conectarse en la red Mesh:

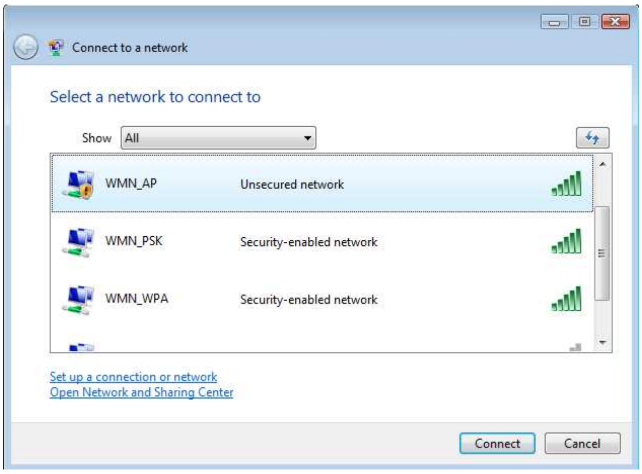


Figura 5-29 SSIDs disponibles para un usuario móvil Mesh en la FIEC

El usuario se enganchará al SSID WMN_AP, como se mencionó es uno de los tres SSIDs asignados en el servidor NOSS, con el cual se inicia el proceso de autenticación a través del túnel ID entre el Gateway 7250 hasta el servidor NOSS por medio del "pool" de direcciones IP que comprende de la IP 10.3.1.1 hasta la IP 10.3.1.50 que son configuradas en el servidor DHCP:

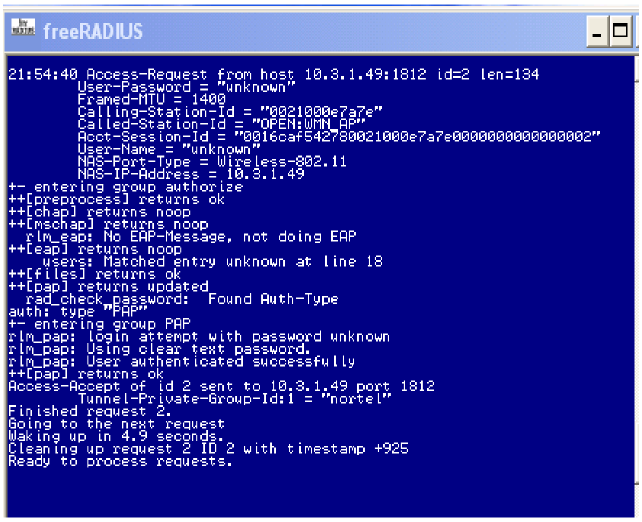


Figura 5-30 Autenticación del servidor RADIUS para la red de la FIEC

Una vez finalizado el proceso de autenticación, se establece la comunicación con el servidor DHCP a través del mismo túnel ID, del cual obtiene la dirección IP para el usuario móvil por medio del punto de acceso virtual VAP. En la siguiente ventana se muestra el proceso de asignación de la dirección IP 10.8.1.3:

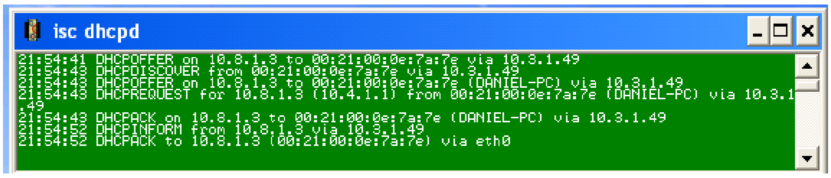


Figura 5-31 Asignación de la dirección IP servidor DHCP para un usuario móvil

La respuesta con la dirección IP asignada que envía el servidor DHCP regresa por el túnel ID y se comunica con el Gateway 7250, que a su vez enruta la información de respuesta hacia el punto de acceso AP@NAP y finalmente a través del enlace de acceso el usuario recibe la información para completar el proceso de autenticación.

Para comprobar que la validación ha sido un éxito, el usuario final deberá tener un mensaje que indica que se encuentra conectado al SSID con el cual se identificó, tal como se muestra en la figura siguiente:

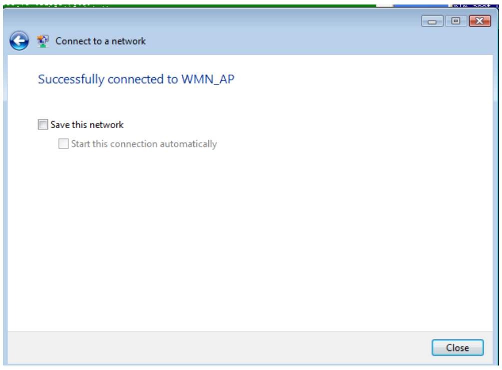


Figura 5-32 Conectividad de un usuario móvil al SSID de la red Mesh

5.5 PRUEBAS DE CONECTIVIDAD

La pruebas que se detallarán a continuación mostrarán la conectividad que existe entre cada uno de los elementos de la red Mesh.

El protocolo ICMP permitirá identificar la conexión con los respectivos tiempos de respuesta, así como también verificar mediante tabla ARP la conectividad física entre los equipos.

5.5.1 CONECTIVIDAD ENTRE EL GATEWAY 7250 Y EL SERVIDOR NOSS

Para habilitar la prueba por protocolo ICMP o también conocida por “Ping” se debe escoger la ruta **Admin> Tools**, como dirección destino se coloca la IP del servidor NOSS y como dirección fuente se coloca la IP de la interface LAN privada, tal como se muestra en la figura 5-33:

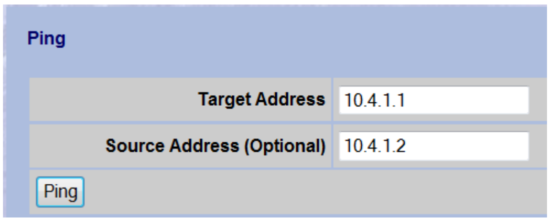


Figura 5-33 Ingreso de direcciones IP para pruebas entre el Gateway y el NOSS

El resultado de la prueba indica que no se presenta pérdida de conectividad y los tiempos de respuesta son menor de 16ms garantizando la estabilidad del servicio, tal como se indica a continuación:

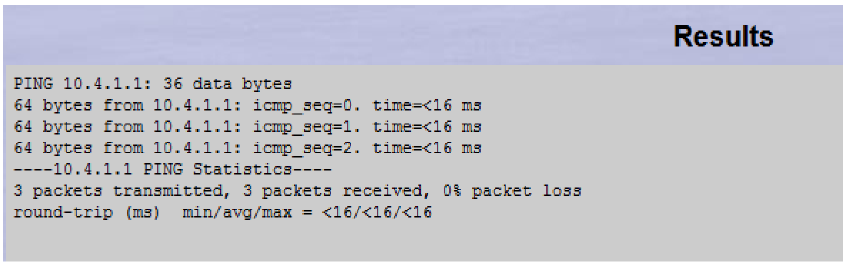
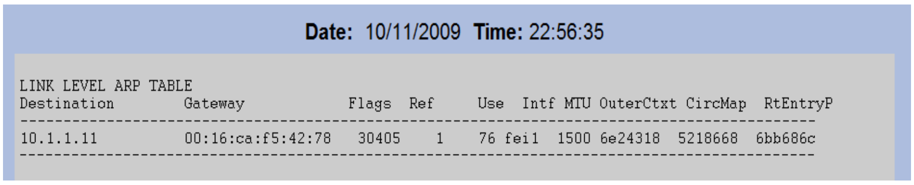


Figura 5-34 Ping realizado desde el Gateway hacia el Servidor NOSS

5.5.2 CONECTIVIDAD ENTRE EL GATEWAY 7250 Y EL PUNTO DE ACCESO AP@NAP

El protocolo ARP crea una tabla con los equipos conectados directamente al Gateway 7250, en la que se toma como información la dirección IP y la dirección MAC.

En la figura que se muestra a continuación podemos identificar que el equipo AP@NAP tiene como dirección IP **10.1.1.11** y como dirección MAC **00:16:ca:f5:42:78** información que se puede comprobar al ingresar por telnet al equipo AP@NAP:



Date: 10/11/2009 **Time:** 22:56:35

LINK LEVEL ARP TABLE

Destination	Gateway	Flags	Ref	Use	Intf	MTU	OuterCtxt	CircMap	RtEntryP
10.1.1.11	00:16:ca:f5:42:78	30405	1	76	fei1	1500	6e24318	5218668	6bb686c

Figura 5-35 Tabla ARP de la interface LAN pública del Gateway 7250

5.5.3 CONECTIVIDAD ENTRE EL GATEWAY 7250 Y UN USUARIO MÓVIL

Por protocolo ICMP podemos establecer conectividad entre el Gateway 7250 y la dirección IP que el servidor DHCP asignó al usuario móvil. En este caso el usuario final está identificado con la dirección IP **10.8.1.3**, tal como se comprobó en el proceso de autenticación:

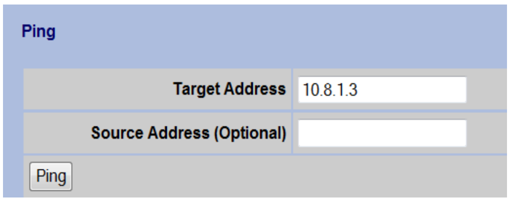


Figura 5-36 Ingreso de dirección IP para pruebas entre el Gateway y el usuario móvil

La prueba indica que a pesar de que los equipos no están conectados físicamente por un cable Ethernet y existe un equipo de por medio que es el punto AP@NAP, ésta no presenta pérdidas de paquetes y los tiempos de respuesta son menor de 16ms, tal como se indica en la figura:

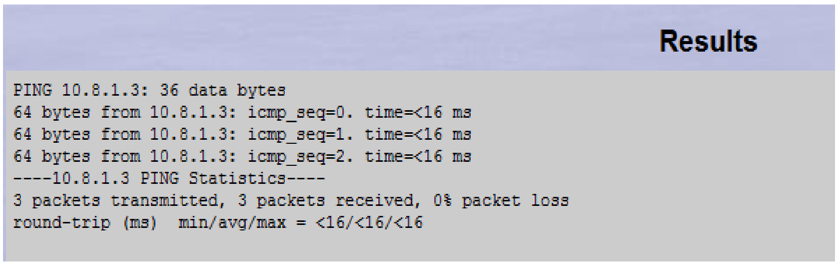


Figura 5-37 Ping realizado desde el Gateway hacia el usuario móvil

5.5.4 CONECTIVIDAD ENTRE LOS PUNTOS DE ACCESO

La funcionalidad del enlace de tránsito TL se identifica con la conectividad entre dos puntos de acceso. Esta prueba establece la conexión entre el punto de acceso AP@NAP que es un equipo AP7220 y un punto de acceso Standalone que es un equipo AP7215.

Para comprobar la conectividad se debe verificar algunos parámetros que son importantes, donde debemos conocer la dirección MAC del enlace de tránsito de los puntos de acceso para colocarlos en los puntos de acceso vecinos, seleccionar el mismo canal del enlace preferible en el canal 152.

Una vez ingresados estos parámetros se inicia una sesión telnet al puerto 2003 para ejecutar la herramienta Site Survey, tal como se muestra en la gráfica:

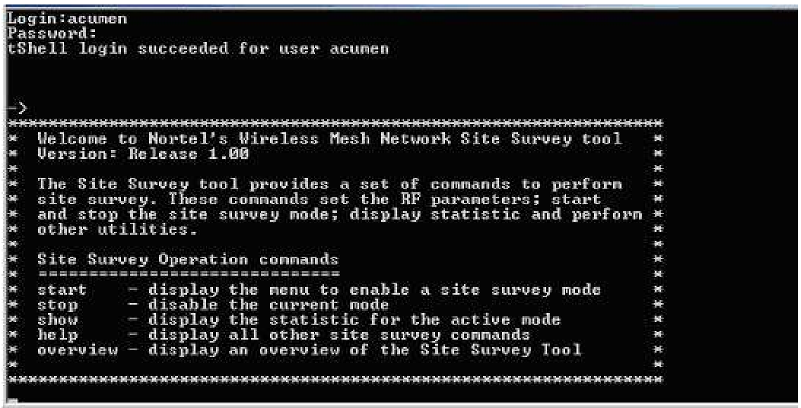


Figura 5-38 Herramienta Site Survey de los puntos AP 7220 y AP 7215

A partir de esto, se inicia el proceso de transmisión en un punto y el proceso de recepción en el otro punto, donde obtenemos los siguientes resultados del equipo que recibe las tramas:

```
-> start
Site Survey Start Menu
======================

1 Continuous TX Mode
2 Continuous RX Mode - fix beam
3 Continuous RX Mode - beam search
4 Link TX Mode
5 Link RX Mode
6 Promiscuous Mode
Press number<CR> to start the mode or h<CR> for help: 2
value = 0 = 0x0
->
Switching to Continuous RX Mode
Expecting site survey frames

-> rxShow

Rate:           6Mb/s   8Mb/s   12Mb/s  18Mb/s  24Mb/s  36Mb/s  48Mb/s  54Mb/s
-------------------------------------------------------------------------------
Good frames :   0       0       0       0       0       0       0       640

Average RSSI:   0       0       0       0       0       0       0       65

Maximum RSSI:   0       0       0       0       0       0       0       77

Minimum RSSI:   0       0       0       0       0       0       0       59

Last RSSI   :   0       0       0       0       0       0       0       66

value = 1 = 0x1
-> stop
```

Figura 5-39 Proceso de recepción de tramas de la herramienta Site Survey del punto AP 7220

Con esta prueba se verifica que se reciben todas las tramas sin pérdidas con el rendimiento máximo del enlace a 54 Mbps.

Adicional se puede verificar la pérdida de paquetes del enlace de tránsito en el modo de recepción a diferentes tasas de capacidad de ancho de banda, donde se obtuvo los siguientes resultados:

```
Press number<CR> to start the mode or h<CR> for help: 5
Expecting 100 frames per rate
If the frames expected is not correct stop the mode
and set the frames expected using the rxNumSet command
value = 0 = 0x0
->
Switching to Link RX Mode
Expecting site survey frames

Rate:           6Mb/s   8Mb/s   12Mb/s  18Mb/s  24Mb/s  36Mb/s  48Mb/s  54Mb/s
-------------------------------------------------------------------------------
Good frames :   100     100     100     100     100     100     100     100

Percent Loss:   0.0     0.0     0.0     0.0     0.0     0.0     0.0     0.0

Average RSSI:   49      49      49      49      49      48      46      46

Maximum RSSI:   51      51      51      51      51      50      48      47

Minimum RSSI:   38      49      49      49      49      48      46      45

Last RSSI   :   50      50      49      50      49      49      47      45

Switching to Idle Mode
_
```

Figura 5-40 Prueba de tramas perdidas del punto AP 7220

Finalizadas estas pruebas verificamos que los dos puntos de acceso trabajan con normalidad y al máximo rendimiento, comprobando la operatividad del enlace de tránsito de los equipos.

5.5.5 CONECTIVIDAD ENTRE DOS USUARIOS DE LA RED MESH

Al establecer la conectividad entre dos usuarios finales, primero cada usuario debe autenticarse por medio del servidor DHCP, el cual asignó la dirección IP **10.8.1.3** al primer usuario identificado y el segundo usuario enganchado tiene asignado la dirección IP **10.8.1.6**. La ventana que presenta el servidor DHCP muestra la información que se ha descrito:

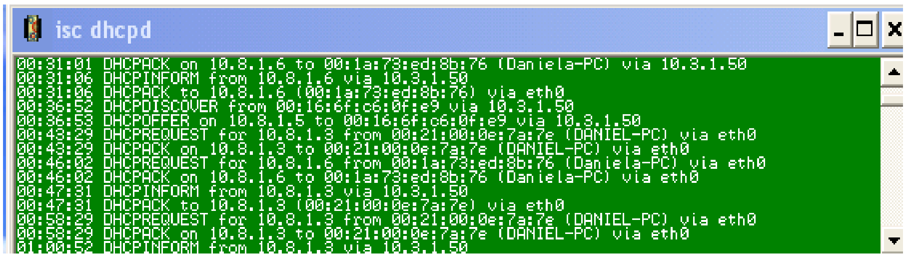


Figura 5-41 Autenticación de dos usuarios móviles en el servidor DHCP

Para las pruebas de conectividad entre los usuarios o equipos terminales se utilizó el protocolo ICMP. Cabe recalcar que con la ayuda del software **Wireless Network Meter** se puede verificar el SSID al cual se conectó el equipo y la dirección IP que tiene asignada la interface inalámbrica.

A continuación se muestran las pruebas realizadas donde se puede verificar que los tiempos de respuesta son en promedio de 8ms y sin pérdidas de paquetes:

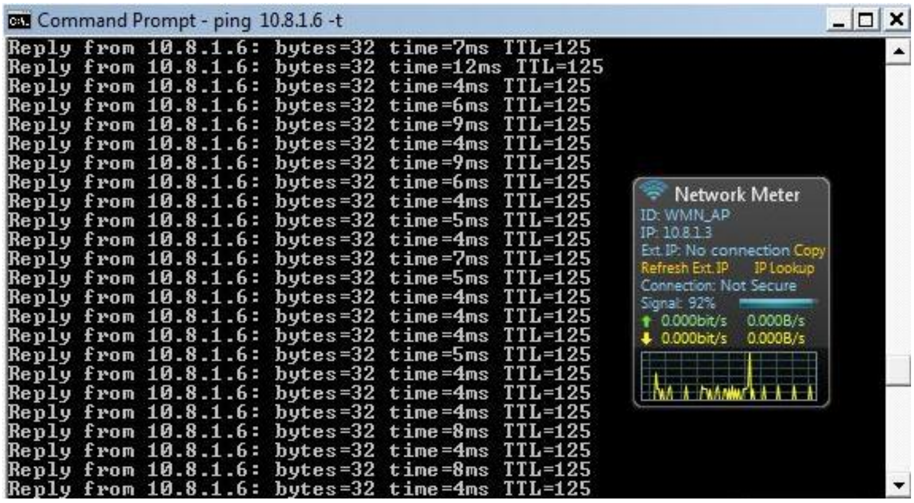


Figura 5-42 Prueba de conectividad desde el usuario 10.8.1.3 hacia el usuario 10.8.1.6

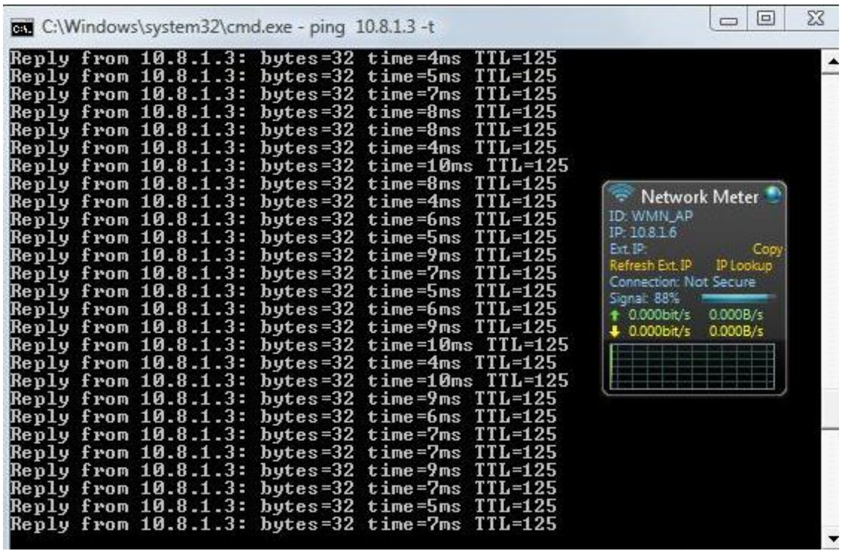


Figura 5-43 Prueba de conectividad desde el usuario 10.8.1.6 hacia el usuario 10.8.1.3

5.5.6 CONECTIVIDAD DE USUARIOS HACIA EL INTERNET

Para probar la conectividad se configura la opción de NAT en el router de borde, así como la opción de dominio DNS del archivo dhcpd.conf del servidor NOSS. Las pruebas realizadas fueron con dos proveedores, con los cuales se tenía la siguiente información:

Ecuanet con red 157.100.92.8 / 29 y DNS 157.100.1.2.

Easynet con red 200.125.200.96 / 29 y DNS 200.125.192.3.

Con esto se comprobó desde una laptop que el acceso hacia las páginas de Internet no mostraron lentitud ni problemas al cargar los elementos como se observa en la figura:

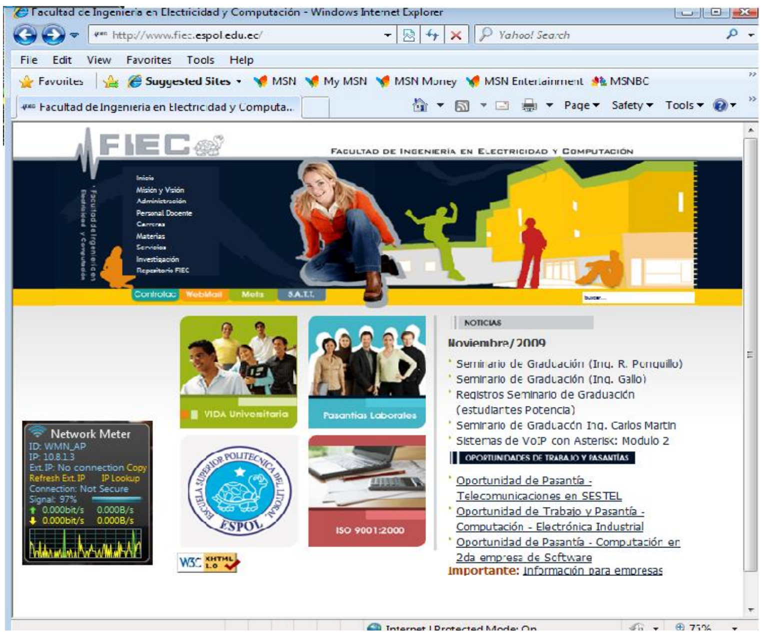


Figura 5-44 Conectividad hacia el Internet desde una laptop

Adicional a las pruebas realizadas desde la laptop también se realizaron desde un teléfono celular y sobre una agenda palm, donde el acceso hacia el Internet se comportaba con cierta lentitud al abrir páginas Web con un ancho de banda alto debido al procesamiento que tienen los equipos aunque no se consideró como un inconveniente para el servicio del usuario.

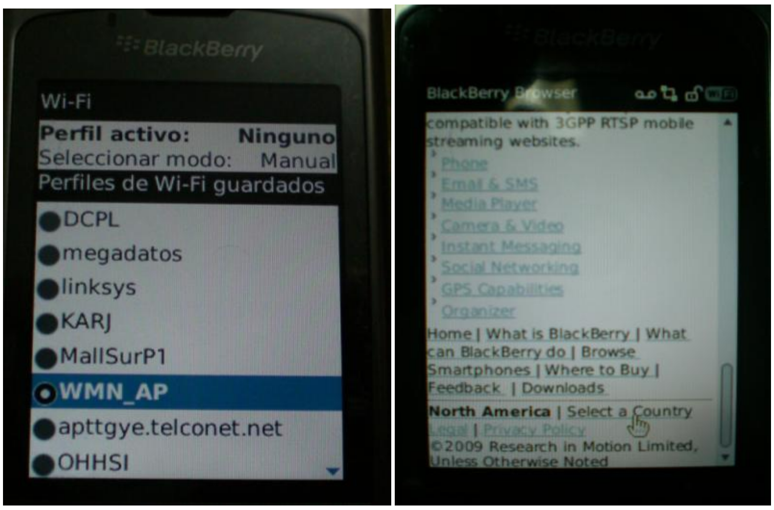


Figura 5-45 Conectividad hacia el Internet desde un teléfono celular

5.6 MEDICIÓN DE LA POTENCIA DE RECEPCIÓN DE UN USUARIO CON RESPECTO A LA DISTANCIA DEL PUNTO DE ACCESO AP

A continuación se detalla de forma gráfica los resultados de las pruebas del enlace de acceso de cada AP 7220 de Nortel. Con las pruebas mencionadas se estimó la cobertura real de la red diseñada midiendo la potencia de recepción del usuario mediante el software Network Meter y pruebas de ping.

Pruebas con el AP@NAP:

Entrada posterior del edificio central de la FIEC:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 80 %.

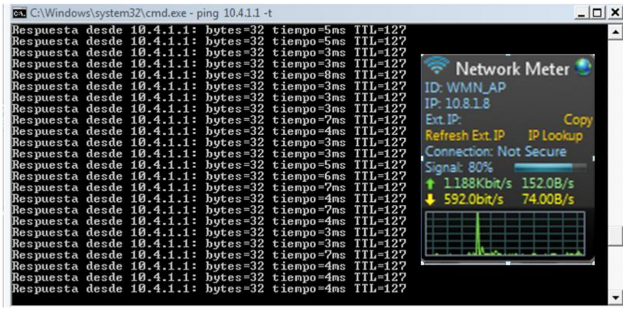


Figura 5-46 Pruebas desde la entrada posterior del edificio central de la FIEC

Area verde límite con el ICM:

Buen tiempo de respuesta, un paquete perdido.

Potencia de señal de recepción, 83 %.

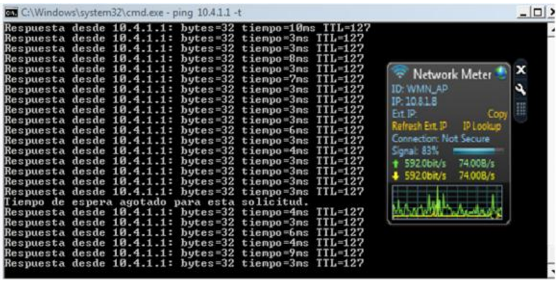


Figura 5-47 Pruebas desde el área verde límite con el ICM

Parqueadero de la FIEC:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 26 %.

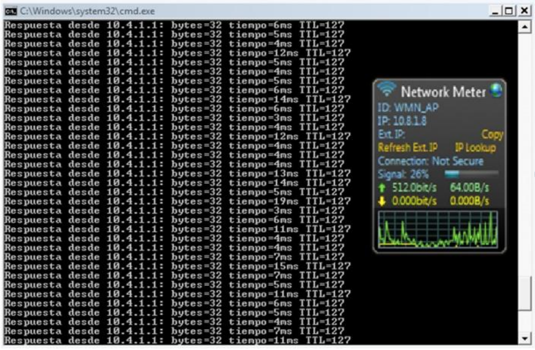


Figura 5-48 Pruebas desde el parqueadero de la FIEC

Límite con Facultad de Mecánica:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 32 %.

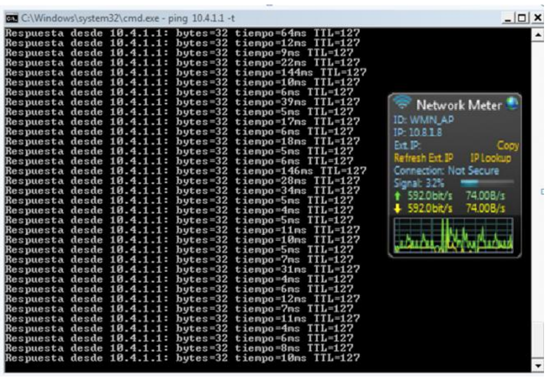


Figura 5-49 Pruebas desde el límite con Facultad de Mecánica

Fuera del Laboratorio de Computación de la FIEC.

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 60 %.

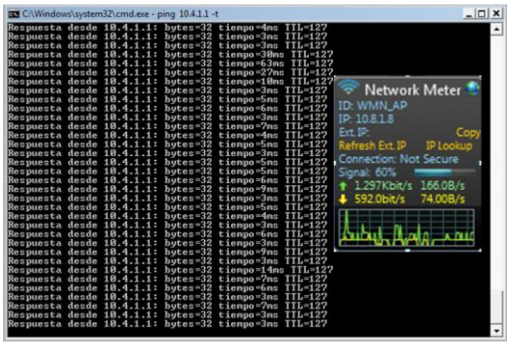


Figura 5-50 Pruebas desde fuera del Laboratorio de Computación de la FIEC

Dentro del Laboratorio de Computación de la FIEC.

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 30 %.

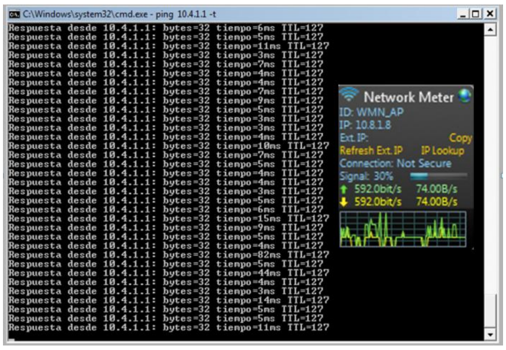


Figura 5-51 Pruebas desde dentro del Laboratorio de Computación de la FIEC

<u>Pruebas con el AP1:</u>

Cancha de Futbol de Ingeniería:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 26 %.

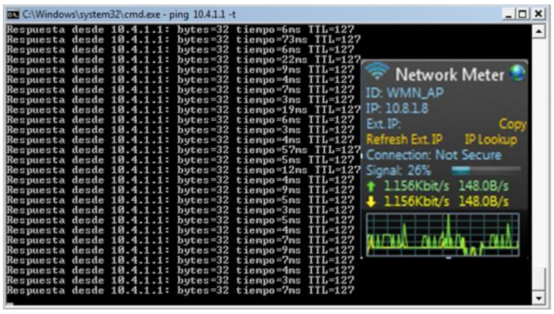


Figura 5-52 Pruebas desde la cancha de Futbol de Ingeniería

Pruebas con el AP2:

Límite con la Facultad de Mecánica:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 20 %.

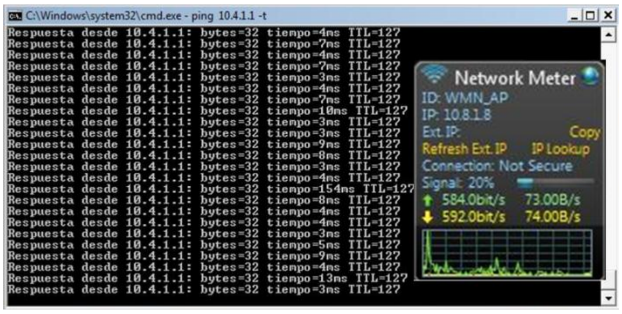


Figura 5-53 Pruebas desde límite con la Facultad de Mecánica

Pruebas con el AP3:

Gimnasio de Profesores:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 20 %.

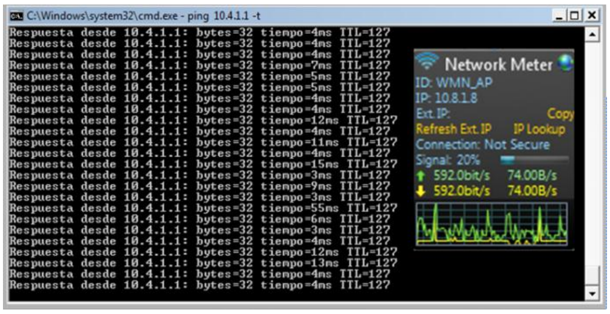


Figura 5-54 Pruebas desde el gimnasio de Profesores

<u>Pruebas con el AP4:</u>

Centro de Ciencias de la Tierra:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 64 %.

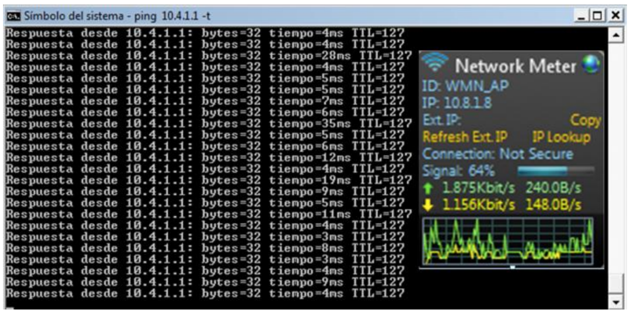


Figura 5-55 Pruebas desde el centro de Ciencias de la Tierra

Dentro del aula de la IEEE:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 28 %.

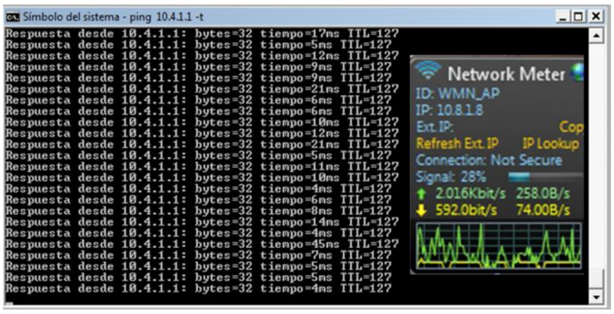


Figura 5-56 Pruebas desde dentro del aula de la IEEE

<u>Pruebas con el AP5:</u>

Bloque de aulas de la FIEC, límite con Mecánica:

Buen tiempo de respuesta, no tiene perdida de paquetes.

Potencia de señal de recepción, 32 %.

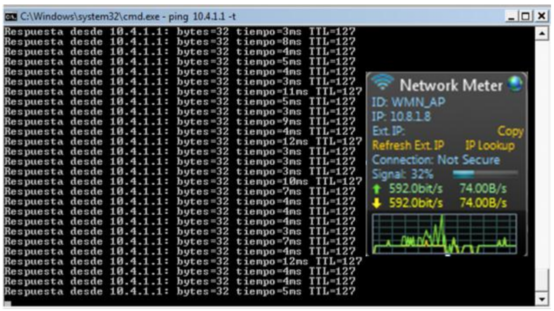


Figura 5-57 Pruebas desde el bloque de aulas de la FIEC, límite con Mecánica

5.7 COMPARACIÓN DE COBERTURA TEÓRICA, SIMULADA Y REAL DE UN PUNTO DE ACCESO

Para calcular la cobertura real de cada AP se utilizo el Windows Command Prompt y el Wireless Network Meter, a continuación se muestra la interfaz usuario que aplican las herramientas mencionadas:

Figura 5-58 Wireless Network Meter

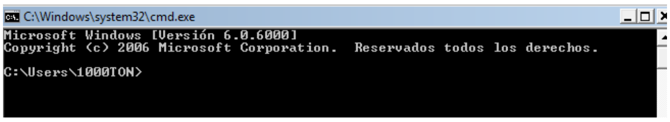


Figura 5-59 Windows Command Prompt

Éstas aplicaciones son útiles para demostrar o verificar las zonas muertas por cada AP.

Los resultados teóricos, simulados y reales se presentan a continuación para cada AP planteado en el diseño:

AP@NAP

Figura 5-60 Cobertura teórica del AP@NAP

Figura 5-61 Cobertura simulada del AP@NAP

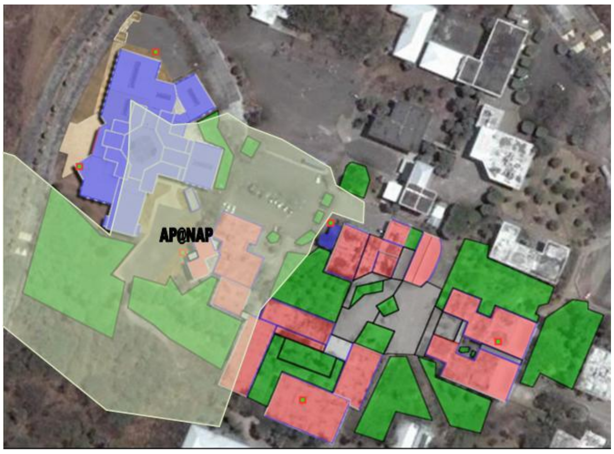


Figura 5-62 Cobertura real del AP@NAP

AP1

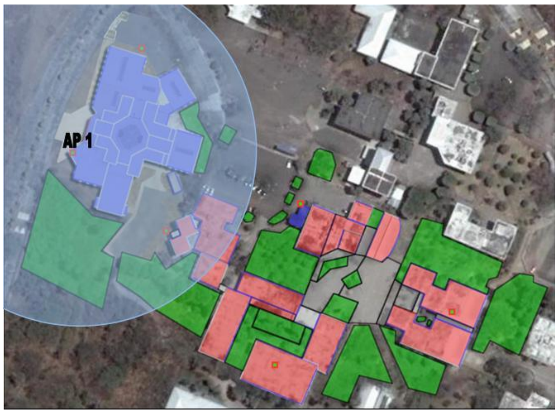


Figura 5-63 Cobertura teórica del AP1

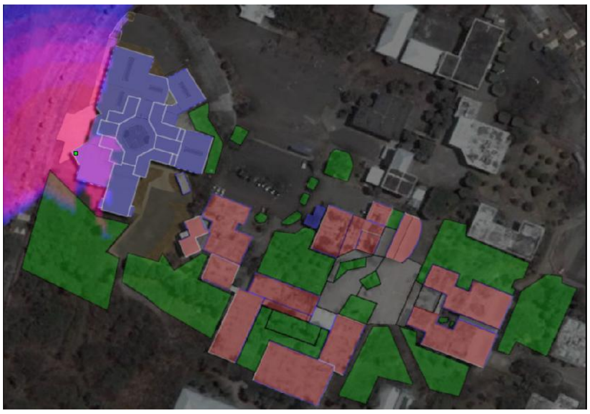


Figura 5-64 Cobertura simulada del AP1

Figura 5-65 Cobertura real del AP1

AP2

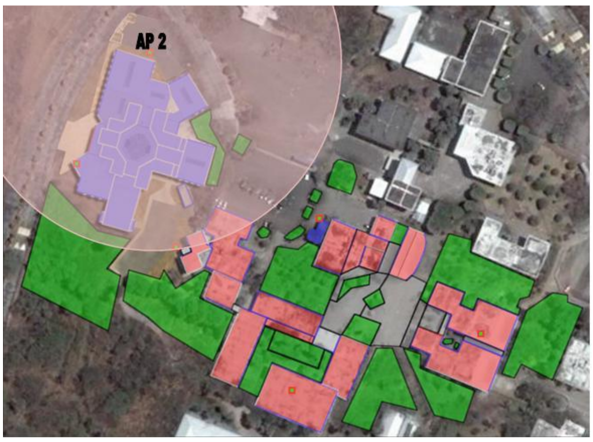


Figura 5-66 Cobertura teórica del AP2

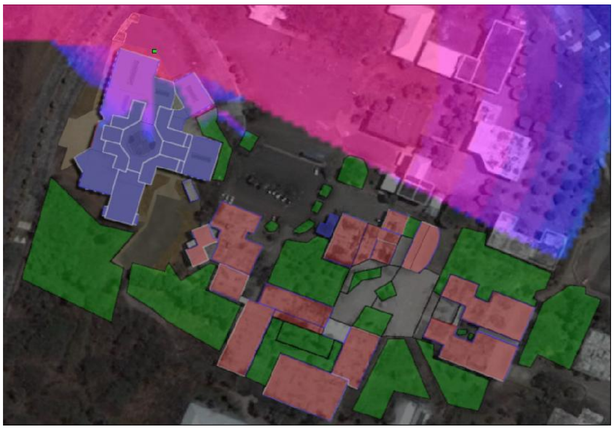


Figura 5-67 Cobertura simulada del AP2

Figura 5-68 Cobertura real del AP2

AP3

Figura 5-69 Cobertura teórica del AP3

Figura 5-70 Cobertura simulada del AP3

Figura 5-71 Cobertura real del AP3

AP4

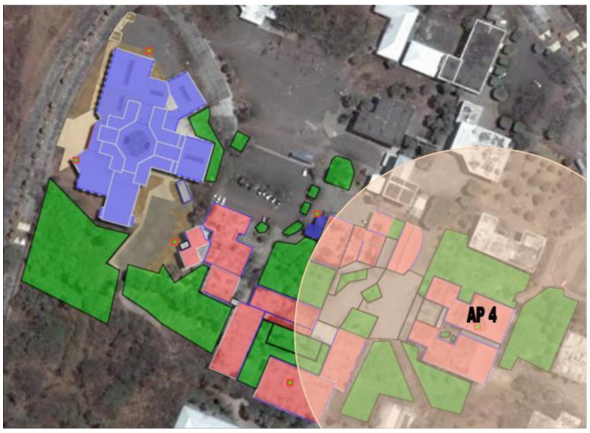


Figura 5-72 Cobertura teórica del AP4

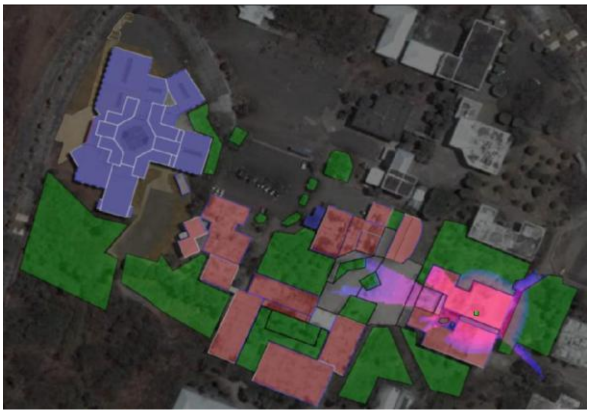


Figura 5-73 Cobertura simulada del AP4

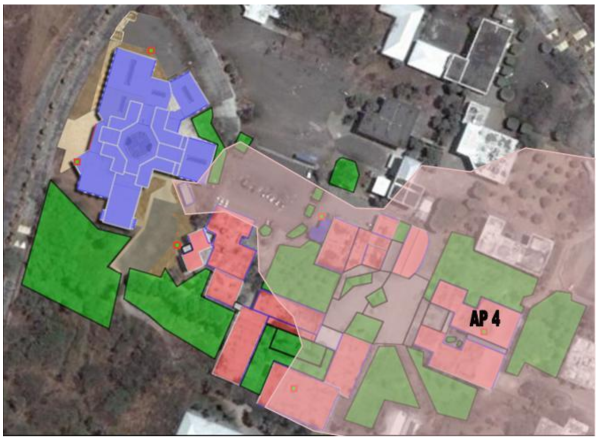


Figura 5-74 Cobertura real del AP4

AP5

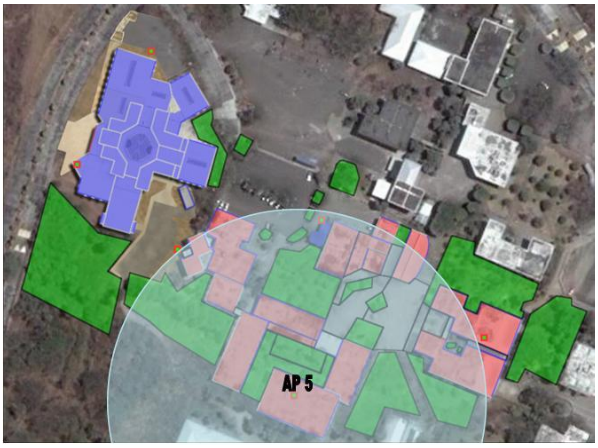


Figura 5-75 Cobertura teórica del AP5

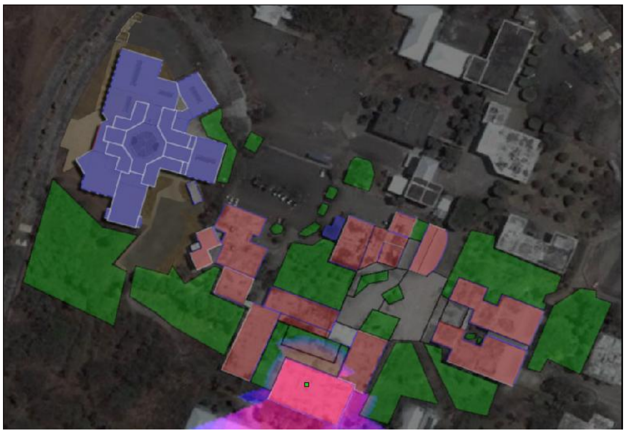


Figura 5-76 Cobertura simulada del AP5

Figura 5-77 Cobertura real del AP5

Como muestran las figuras anteriores los resultados teóricos y reales son similares, pero no así los simulados por varios motivos:

- Las áreas verdes en el Planner se consideraron zonas muy densas y como un bloque de una sola altura.

- Para marcar los límites de cada zona el Planner sólo permite cuatro opciones, Foliage, Windowed External Wall, Windowless External Wall y Blocking Boundary; para el caso de la FIEC solo se aplicó el Windowed External Wall con una atenuación de 6.9 dB y el Windowless External Wall con una atenuación de 15 dB, cuyas atenuaciones como se demuestra en las figuras anteriores son exageradas para el ambiente real de la FIEC.

- La facultad se encuentra en un ambiente donde existen muchos desniveles que a pesar de haberlos considerado, se notó un margen de error considerable en la simulación.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Wireless Mesh Networks ha sido implementada en ciudades y universidades satisfaciendo las exigencias de los usuarios, puesto que posee una infraestructura robusta, flexible e innovadora. Además de poseer la capacidad tener redundancia y permitir la autoreparación de rutas.

2. El diseño de la red mesh para la Facultad de Ingeniería en Electricidad y Computación se planteo basándose a los siguientes puntos:

    - Que exista no más de 200 metros entre APs.

- Cada AP tiene una cobertura de 100 metros a la redonda.

Considerando lo anterior, el diseño de la red mesh para la FIEC debe tener mínimo 5 APs y un AP@NAP.

3. La topología diseñada para la Wireless Mesh Network de la FIEC se basa en rendimiento, con esto se logró evitar que se formen cuellos de botella ocasionados por subárboles.

4. En los resultados de la simulación del diseño teórico se notó varias “zonas muertas”, por lo cual se realizó una nueva simulación aumentando tres puntos de acceso, con esto se logró reducir el área de estas zonas, cabe recalcar que las mencionados áreas se ubican en lugares donde existe vegetación por ende es poco probable encontrar usuarios.

5. Comparando los resultados entre teóricos y simulados se obtuvo un error de 3 puntos de acceso; además tanto la simulación del diseño teórico como el diseño mejorado se observó gran intensidad de la señal en los lugares considerados de mayor concentración de usuarios.

6. Se realizaron pruebas reales con un punto de acceso AP 7220 de Nortel ubicado en cada uno de los lugares planteados en el diseño

teórico, obteniendo en la mayoría de los casos más de la cobertura de 100 metros reconocida como estándar.

7. Se confirmó que los equipos que pertenecen al diseño de la red Mesh de Nortel son de fácil instalación y de realizar mantenimientos periódicos. Se promedió una hora por la instalación de cada punto.

8. Se comprobó que mediante las configuraciones realizadas en cada uno de los equipos de la red mesh de Nortel, se pudo realizar las diversas pruebas de conectividad como son:

   - Conectividad entre puntos de acceso.
   - Conectividad entre el usuario y la puerta de enlace Gateway 7250.
   - Conectividad de la puerta de enlace y los puntos de acceso hacia el servidor NOSS.

9. Se realizó pruebas de navegación hacia el Internet mediante el uso de un router de borde, obteniendo excelentes resultados. Se logró proveer de servicio a 2 laptops, 1 palm y 2 teléfonos celulares. Cabe recalcar que las pruebas se realizaron con varios proveedores de Internet y un ancho de banda de 512kbps obteniendo resultados de tiempos de respuesta similares.

10. Al finalizar el proyecto se pudo notar que los resultados teóricos y reales son similares, no así los resultados simulados por varios motivos entre los cuales resaltan:

    - En el simulador se consideró a las áreas verdes como un solo bloque de una sola altura obteniendo una área demasiado densa lo cual no es lo que existe en realidad en la Facultad de Ingeniería en Electricidad y Computación

    - La FIEC por estar ubicada en un zona montañosa presenta muchos desniveles que a pesar de haberlos considerado, no fue suficiente para plasmar el ambiente de forma virtual en el simulador.

11. Se logró disminuir el número de puntos de acceso y aumentar la cobertura a un 100% del área de la FIEC en comparación con la infraestructura actual de la Facultad.

12. Mediante pruebas se observó que no existían pérdidas de paquetes al momento de que un usuario se traslade de un punto a otro es decir se demostró la capacidad de movilidad que le brinda la red a los usuarios.

13. Aunque el presupuesto total para la implementación de la red se aprecie elevado, su valor se lo considera justo por las diversas

ventajas que brinda esta infraestructura como la facilidad de expandirse de manera fácil y rápida. Se calcula que en corto plazo exista mayor competencia entre fabricantes de equipos para soluciones Mesh con lo cual los valores por equipos disminuirían considerablemente.

Recomendaciones

1. Se recomienda establecer el uso de un software de monitoreo de los puntos de acceso, para que en caso de que exista pérdida de comunicación hacia un equipo, exista un tiempo de respuesta oportuna al solucionarlo.

2. Se recomienda realizar Upgrades (actualizaciones) de manera periódica, para asegurar que los equipos trabajen con el mejor rendimiento empleando el menor procesamiento y asegurar al usuario un servicio sin problemas.

3. En caso de querer ampliar la cobertura de la red se recomienda realizar la instalación de los nuevos puntos de acceso en la parte alta de las edificaciones o en postes considerando ubicarlos a no más de 10 metros sobre el nivel del piso, y a una distancia entre cada equipo no menor de 200 metros y no mayor a 800 metros.

4. Para el diseño de nuevas redes Mesh se recomienda que el direccionamiento IP que se aplique, sea realizado segmentando redes de clase C de una red privada, para facilitar el enrutamiento y asegurar la comunicación entre las interfaces de los equipos de infraestructura.

5. Cuando se desee simular con ayuda del Planner una nueva propuesta de diseño Mesh, se debe tomar como referencia un plano o una foto de vista aérea tomada perpendicular a la superficie para asegurar que los resultados que se obtengan tengan el menor margen de error posible.

6. Para evitar saturación de los enlaces de tránsito por la cantidad de usuarios navegando de manera simultánea hacia el Internet es recomendable obtener un servicio con ancho de banda mayor de 2Mbps, ya que se tiene un gran número de usuarios, los cuales realizan descargas de información y comparten archivos.

7. Se recomienda la instalación del servidor NOSS sobre el sistema operativo Windows XP, para evitar problemas en el comportamiento del servidor por incompatibilidad. En caso de tener otro sistema operativo se puede instalar Windows XP sobre una máquina virtual.

Perspectivas Futuras

Las WMN han sido implementadas en países como Estados Unidos, México y España, solucionando las necesidades de comunicación de los usuarios en campus universitarios y comunidades, los resultados de esta solución y opiniones de expertos han sido positivos.

Entre las empresas internacionales conocidas que han dedicado tiempo y dinero al desarrollo de ésta tecnología tenemos a Nortel, Cisco y Motorola, en la actualidad las empresas mencionadas tienen entre sus soluciones de telecomunicaciones a las redes malladas promocionando una variedad de productos mesh.

En el Ecuador varias empresas proveedoras de servicios de telecomunicaciones conocen la tecnología pero no arriesgan su capital por desconfianza a la aceptación del usuario. La empresa que ha tratado de introducir los equipos mesh en nuestro país es Nortel pero no ha tenido buenos resultados por lo mencionado en líneas anteriores, el miedo de las empresas a mejorar e innovar su infraestructura.

A nivel mundial se está observando una tendencia hacia la tecnología mesh puesto que los usuarios de las redes tienen más necesidades y son más exigentes, es por esto que se estima que en el Ecuador en poco tiempo habrá más proyectos y propuestas de soluciones mesh y con esto la motivación de las empresas grandes de telecomunicaciones en nuestro país para considerar invertir en un proyecto mesh innovador y con grandes ventajas. Además una vez implementada la solución se crearán en el Ecuador nuevos modelos de negocios y fuentes de trabajo enriqueciendo la economía del país.

Cabe recalcar que un país con soluciones mesh implementadas no solo gana en el campo económico, sino también en el aspecto de seguridad y rapidez en respuestas a las emergencias.

ANEXO A

FORMATO DEL MENSAJE RREQ

El mensaje RREQ se envía para solicitar una ruta hacia un determinado nodo destino. El formato de este mensaje es el siguiente:

0	8					13	24 31
Tipo	J	R	G	D	U	Reservado	Cuenta de Saltos
RREQ ID							
Dirección IP Destino							
Número de Secuencia Destino							
Dirección IP Fuente							
Número de Secuencia Fuente							

A continuación de detalla cada uno de los puntos que conforman la estructura básica del mensaje RREQ:

Tipo: Indica el tipo del paquete, en este caso tiene un valor de 1.

J: Join Flag o Bandera de Unión; reservada para Multicast.

R: Repair Flag o Bandera de Restablecimiento; reservada para Multicast.

G: Flag Gratuito; indica si debe enviarse un RREP en modo Unicast al nodo especificado por el campo dirección IP destino.

D: Bandera Únicamente Destino, la cual indica que sólo el destino puede responder a este mensaje RREQ.

U: Número de Secuencia Desconocido, indica que el número de secuencia es desconocido.

Reservado: Campo reservado, inicializado a 0 para ignorar la recepción.

Contador de saltos: Hop Count; es el número de saltos desde el nodo fuente hasta el nodo destino.

RREQ ID: Número de secuencia identificado en conjunto con la dirección IP del nodo fuente.

Dirección IP Destino: Indica la dirección IP del nodo solicitado.

Número de Secuencia Destino: Último número de secuencia recibido en la fuente de cualquier ruta hacia el destino.

Dirección IP Fuente: Dirección IP del nodo el cual originó el RREQ.

Número de Secuencia Fuente: Número de secuencia actual del nodo origen.

ANEXO B

FORMATO DEL MENSAJE RREP

El mensaje RREP se envía como contestación a un RREQ confirmando un establecimiento de ruta. Sigue el formato siguiente:

<table>
<tr><td>0</td><td>8</td><td>9</td><td>10</td><td>19</td><td>24 31</td></tr>
<tr><td>Tipo</td><td>R</td><td>A</td><td>Reservado</td><td>Tamaño de Prefijo</td><td>Cuenta de Saltos</td></tr>
<tr><td colspan="6">Dirección IP Destino</td></tr>
<tr><td colspan="6">Número de Secuencia Destino</td></tr>
<tr><td colspan="6">Dirección IP Fuente</td></tr>
<tr><td colspan="6">Tiempo de Vida</td></tr>
</table>

A continuación de detalla cada uno de los puntos que conforman la estructura básica del mensaje RREP:

Tipo: Indica el tipo del paquete, en este caso es igual a 2.

R: Join Flag o Bandera de Restablecimiento; reservada para Multicast.

A: Bandera de Reconocimiento (Acknowledgment); se comprueba si un enlace es unidireccional.

Reservado: Campo reservado, inicializado a 0 para ignorar la recepción.

Tamaño de Prefijo: Especifica que el próximo salto indicado puede ser utilizado para cualquier nodo con el mismo prefijo de enrutamiento, siempre que no tenga el valor de cero.

Contador de saltos: Número de saltos desde el nodo fuente hasta el destino.

Dirección IP Destino: Indica la dirección IP del nodo solicitado.

Número de Secuencia Destino: Último número de secuencia destino recibido por el nodo fuente, para cualquier ruta hacia algún destino.

Dirección IP Fuente: Dirección IP del nodo, el cual originó el RREQ.

Tiempo de Vida (TTL): Lifetime; tiempo de vida en milisegundos, para que los nodos que reciben un RREP consideren una ruta válida.

ANEXO C

FORMATO DEL MENSAJE RERR

0	8	9	24 31
Tipo	N	Reservado	Cuenta Destino
Dirección IP Destino Inalcanzable			
Número de Secuencia Destino Inalcanzable			
Dirección IP Destino Inalcanzable Adicional			
Número de Secuencia Destino Inalcanzable Adicional			

A continuación de detalla cada uno de los puntos que conforman la estructura básica del mensaje RERR:

Tipo: Indica el tipo del paquete, en este caso es igual a 3

N: El flag de No Borrado (No Delete), indica no suprimir ruta.

Reservado: Campo reservado, inicializado a 0 para ignorar la recepción.

Cuenta Destino: Es el número de destinos inalcanzables que se encuentran en el mensaje. Como mínimo será 1.

Dirección IP Destino Inalcanzable: Dirección IP del destino que se ha convertido en inalcanzable debido a un error en el enlace.

Número de Secuencia Inalcanzable: Número de secuencia en la tabla de enrutamiento para un destino registrado previamente en el campo dirección IP destino inalcanzable.

ANEXO D

FORMATO DEL MENSAJE OLSR

A continuación se presenta el formato del mensaje OLSR:

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Message type</td><td colspan="8">Vtime</td><td colspan="16">Message size</td></tr>
<tr><td colspan="32">Originator address</td></tr>
<tr><td colspan="8">TTL</td><td colspan="8">Hop count</td><td colspan="16">Message sequence number</td></tr>
<tr><td colspan="32">Data ::</td></tr>
</table>

Donde tenemos diferentes valores para el campo de Tipo de Mensaje (Message Type), como se muestra en la siguiente tabla:

Tipo	Mensaje
0	
1	HELLO
2	TC
3	MID
4	HNA
5 - 127	
128 - 255	Mensajes Privados o locales

En lo que respecta al Tipo de Mensaje, a continuación se presenta el formato de los mensajes HELLO y de topología de control TC, que son los mensajes más utilizados:

<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="16">Reserved</td><td colspan="8">Htime</td><td colspan="8">Willigness</td></tr>
<tr><td colspan="8">Link Code</td><td colspan="8">Reserved</td><td colspan="16">Link Message Size</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">..</td></tr>
<tr><td colspan="8">Link Code</td><td colspan="8">Reserved</td><td colspan="16">Link Message Size</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
<tr><td colspan="32">Neighbor Interface Address</td></tr>
</table>

<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="16">ANSN</td><td colspan="16">Reserved</td></tr>
<tr><td colspan="32">Advertised Neighbor Main Address</td></tr>
<tr><td colspan="32">Advertised Neighbor Main Address</td></tr>
</table>

ANEXO E

PROTOCOLO PROACTIVO TBRPF

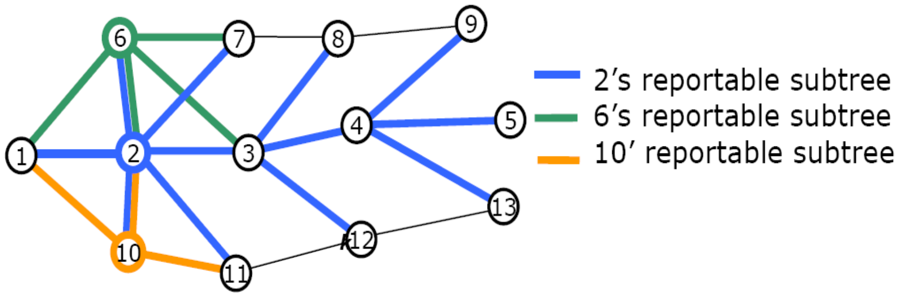
El protocolo TBRPF consta de dos módulos:

- Módulo TND, Neighbor Discovery Module o Módulo de Descubrimiento de Vecinos, quien envía mensajes HELLO que reportan sólo los cambios de los nodos vecinos.

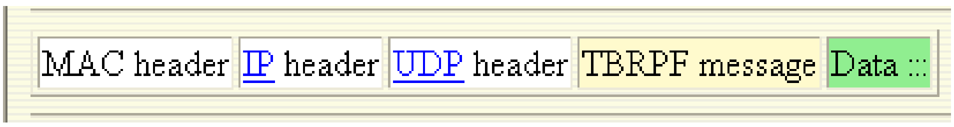
- Routing Module o Módulo de Enrutamiento, que opera basado en información parcial de la topología.

TBRF únicamente propaga las actualizaciones del enlace de estado en dirección reversa al Spanning Tree formado por los caminos de saltos cortos. Sólo los cambios del árbol fuente estarán incluidos en las actualizaciones.

A continuación se presenta un diagrama de red de varios nodos, en el cual se forman varios árboles, los cuales tienen enlace hacia todos los nodos de la red.



Para conocer mejor el formato del mensaje de un protocolo TBRPF, se presenta el siguiente diagrama:



En la cual, dentro del mensaje TBRPF tenemos el formato del mensaje HELLO, que puede ser de tres tipos:

NEIGHBOR REQUEST (TYPE = 2)
NEIGHBOR REPLY (TYPE = 3)
NEIGHBOR LOST (TYPE = 4)

Cada mensaje HELLO tiene el siguiente formato:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   0   | TYPE  |      HSEQ       |  Pri  |          n          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Neighbor Interface Address (1)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Neighbor Interface Address (2)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                              ...                              ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Neighbor Interface Address (n)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Donde HSEQ es un número de 8 bits e indica el número de secuencia del mensaje.

ANEXO F

CONSIDERACIONES AL DISEÑAR LA COBERTURA DEL ENLACE DE ACCESO

<u>PLANIFICACIÓN DEL TAMAÑO DE COBERTURA DE ENLACE DE ACCESO Y DEL NIVEL DE SERVICIO:</u>

Al diseñar el área de cobertura se debe lograr un equilibrio entre las ventajas respecto a grandes zonas de cobertura del enlace de acceso contra el efecto que puede ocasionar en el servicio del usuario.

En la siguiente tabla se muestra las ventajas y desventajas de tener un solo AP 7220 para un área de cobertura grande.

Ventajas	Desventajas
Reduce el número de puntos AP 7220 en la red	El aumento de la distancia del enlace de acceso, reduce la tasa de transmisión de datos de un punto de acceso AP 7220
Simplifica el diseño y el mantenimiento de la red	Al incrementar el número de usuarios, reduce la tasa de transmisión de datos de un punto de acceso AP 7220, ya que se requiere compartir el ancho de banda asignado para toda la red
Disminuye el gasto en materiales	Aumenta el gasto en materiales

PROPORCIONAR LA TASA DE DATOS DEL RENDIMIENTO THROUGHPUT:

La tasa de transmisión para un nodo móvil depende de:

- La distancia entre el nodo móvil y el punto de acceso AP 7220 al que se ha conectado.
- El número de nodos móviles conectados compartiendo el ancho de banda disponible del punto de acceso AP 7220.

FACTORES PARA SELECCIONAR EL TIPO DE ANTENA DEL ENLACE DE ACCESO:

De la elección de la antena a utilizar en los nodos dependen el área de cobertura y el rendimiento de los enlaces de acceso. Los AP 7220 admiten dos opciones para las antenas:

En la siguiente tabla se describe las características de las antenas integradas PIFA y las antenas de Dipolo Externo.

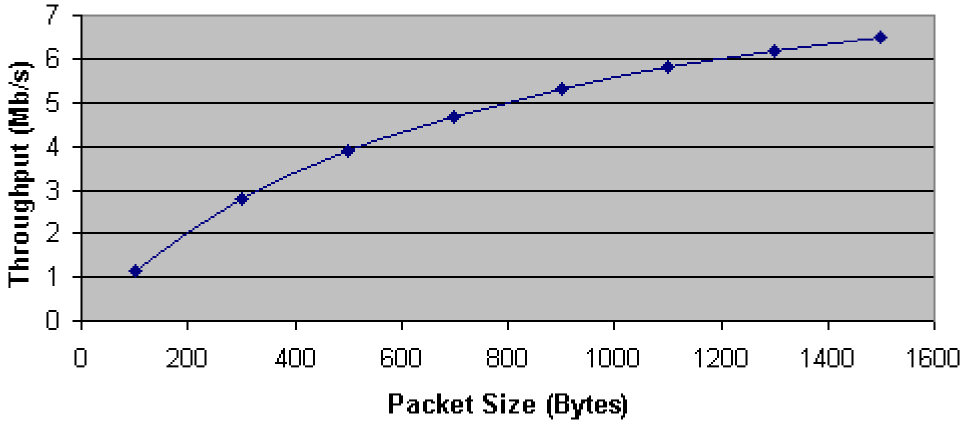
	Antena Integrada PIFA	**Antena de Dipolo Externo**
Ganancia Alternativa	+ 0 dBi	+ 5 dBi
Uso	Donde un AP 7220 debe proporcionar una capacidad de acceso de alta densidad dentro de una área de acceso de un “hotspot”.	Donde un AP 7220 debe proporcionar la máxima área de cobertura, superando obstáculos en un ambiente outdoor o proporcione la máxima penetración en una edificación.
Ventajas	La menor ganancia de la antena permite poco espacio entre ellas, pero sin problemas de interferencia, algo que no ocurre con una antena de ganancia alta.	La mayor ganancia de la antena permite un mayor espacio entre ellos. Tienen mayor potencia para superar los obstáculos o mantener una tasa de transmisión aceptable sobre grandes distancias.
Observaciones	Cualquier obstáculo puede ocasionar reducción de la capacidad del enlace de acceso aunque no necesariamente representa un problema en los "hotspots".	La mayor potencia de radio frecuencias (RF) crea interferencias entre los puntos de acceso vecinos, aunque no sea un problema típico en un espacio de enlace outdoor

ANEXO G

FACTORES QUE LIMITAN LA CAPACIDAD EN UNA RED INALÁMBRICA MESH

TASA DE TRANSMISIÓN DE DATOS DEL ENLACE DE ACCESO:

La máxima capacidad del enlace de acceso en el estándar 802.11b es de 6 Mbps, asumiendo transmisión con paquetes de 1500 bytes. La tasa de transmisión disminuye al aumentar la distancia de los puntos de acceso AP 7220 provocando la reducción de la capacidad. También depende del tamaño del paquete, tal como se muestra en la figura. La capacidad del enlace de acceso se comparte entre el tráfico de bajada (tráfico dirigido desde la red de backbone hacia el nodo móvil) y el tráfico de subida (desde el nodo móvil hacia la red de backbone).



<u>CAPACIDAD Y RENDIMIENTO DE LA RED BACKHAUL:</u>

Cada enlace de tránsito de un punto de acceso AP 7220@NAP puede llevar una carga útil (payload) máxima de 13 Mbps. Al aumentar el número de enlaces de tránsito desplegados a un punto de acceso AP 7220@NAP significa compartir el ancho de banda total del enlace de tránsito, reduciendo el rendimiento de cada enlace de tránsito.

Si la tasa de transmisión de la capa física de un enlace de tránsito es inferior al máximo de 54 Mbps o si existe una retransmisión representativa, entonces el máximo rendimiento del enlace de tránsito disminuye sobre una base proporcional.

Para evitar lo mencionado, se puede aumentar la capacidad mediante el despliegue de múltiples puntos de acceso AP 7220@NAP conectados de manera cableada al Wireless Gateway 7250.

ANEXO H

Dhcpd.conf

A continuación se muestra el archivo de configuración Dhcpd.conf

```
# Archivo: ISC DHCPD
# Release: 2.3
ddns-update-style none;
max-lease-time 3600;
default-lease-time 1800;

# OMAPI (remote queries interface)
omapi-port 7911;
key OMAPI {
	algorithm hmac-md5;
	secret Mh3C9d1kF+tFkxB4g3MugIFsw90fNw==;
}

 omapi-key OMAPI;
```

 # Si el servidor DHCP es el servidor por defecto se habilita el comando "authoritative"

authoritative;

 # Redes para VPN

subnet 0.0.0.0 netmask 255.255.255.0 {

}

 # IPsec subnets – Permite un túnel entre la LAN pública y la LAN privada

subnet 10.3.1.0 netmask 255.255.255.0 {

}

 # Vendor specific, Nortel

option space nosswin;

option nosswin.ospfareaid code 1 = ip-address;

option nosswin.pgaddr code 2 = ip-address ;

option nosswin.ikeauthmethod code 3 = unsigned integer 8 ;

if option vendor-class-identifier = "Nortel" {

vendor-option-space nosswin;

}

 # NOSS Private Subnet 10.4.1.0/24 – Direcciones IP para la LAN Publica

subnet 10.4.1.0 netmask 255.255.255.0 {

}

 # AP Extranet Subnet 10.1.1.0/24 – Direcciones IP para los puntos de acceso AP

subnet 10.1.1.0 netmask 255.255.255.0 {

option nosswin.ospfareaid 10.0.0.0;

option nosswin.pgaddr 10.1.1.1;

```
option nosswin.ikeauthmethod 2;

# Asignamiento dinámico de los puntos APs Standalone
  range 10.1.1.64 10.1.1.254;
  option routers 10.1.1.1;
  option subnet-mask 255.255.255.0;
  filename "ap.ftp";
  server-name "10.4.1.1";
}



# Mobile Users Subnet 10.8.1.0/24 – Direcciones IP para los usuarios móviles
#IP Router de Borde = 10.8.1.254
#DNS Proveedor Internet = 200.125.192.3
subnet 10.8.1.0 netmask 255.255.255.0 {
    range 10.8.1.2 10.8.1.254;
    option routers 10.8.1.254;
    option domain-name-servers 200.125.192.3;
    option ntp-servers 10.4.1.1;
    option mobile-ip-home-agent 10.4.1.2;
    option subnet-mask 255.255.255.0;
}

# ********** FIN del Archivo de Configuración Dhcpd.conf **************
```

ANEXO I

Ap.ftp

A continuación se muestra el archivo de configuración FTP para un AP 7220.

 # Archivo de Configuración NOSSwin FTP Sample R3.0

 # Parámetros de Configuración del servidor RADIUS para los puntos de acceso AP 7220

[radius]

 # Authentication

PrimaryAuthenticationServer=10.4.1.1:1812

PrimaryAuthenticationSecret=SB7nh6dg5t

SecondaryAuthenticationServer=10.4.1.1:1812

SecondaryAuthenticationSecret=SB7nh6dg5t

 # Accounting

PrimaryAccountingServer=10.4.1.1:1814

PrimaryAccountingSecret=SB7nh6dg5t

SecondaryAccountingServer=10.4.1.1:1813

SecondaryAccountingSecret=SB7nh6dg5t

[dhcp]

 # Identificacion del servidor DHCP

WarpPrimaryDhcp = 10.4.1.1

MnPrimaryDhcp = 10.4.1.1

UserClass=class

[dst]

 # Habilita el Dynamic Spanning Tree para auto configuración del enlace TL

dynamicSpanningTreeOff = 0

[pgHa]

 # Se define el mapeo entre las direcciones IP intranet y extranet del WG 7250

 # IPs=interface Pública del WG7250, IP Administración del WG7250

PgAddrAndHaAddr = 10.1.1.1,10.4.1.2

[subscriberGroup]

 # Mapeo entre el tunnel ID= Red de los usuarios, nombre del túnel

MnSubnetAndTunnelId = 10.8.1.0,nortel

MnSubnetAndTunnelId = 10.9.1.0,secure-wpa

MnSubnetAndTunnelId = 10.10.1.0,secure-psk

[accessLink]

 # Habilita el enlace de Acceso de un AP 7220

mode=802.11b

SubnetaddrAndMask= 10.1.1.0,255.255.255.0

Enable=1

#Asignamiento manual del canal

Channel=2

#Nivel de Potencia del enlace de acceso AL

Power=1

#Tiempo de la trama en la cual corre la selección automática del enlace de acceso AL

AutoScanTime=4

[ssid]

 # Configuración para un VAP(Punto de acceso virtual)

 # Parámetro ASCII de máximo 32 caracteres

ssid = WMN_AP

[AccessLinkIp]

 # El AccessLinkIp define la dirección IP del enlace de acceso AL que usara un nodo móvil

AccessLinkIp = 10.8.1.1,255.255.255.0

 # Autenticación de un nodo móvil (enable=1, disable=0)

wpa_eap=0

wpa_psk=0

non_rsna=1

 # BroadcastSsid indica si el SSID debería hacer de broadcast.

#enable=1, disable=0

broadcastSsid = 1

 # AuthType especifica el método usado para generar el username enviado al Radius para nodos

 # móviles no-RSNA o RSNA usando autenticación WPA-PSK

 # 0 = anonymous. El username se setea como UNKNOWN.

 # 1 = MAC-based. El username se setea a la dirección MAC del usuario móvil

 # 2 = SSID. El username se setea al SSID utilizado por el nodo móvil

authType=0

[configManager]

#Archivo de Configuración

ConfigFile=ap.ftp

#Dirección IP del servidor FTP

Server=10.4.1.1

 # Username de la cuenta FTP

Username=nortelWarp

 # Password de la cuenta FTP

Password=nortelWarp

[configure]

#Asignación del área ID para emplear OSPF

OSPFAreaid=10.0.0.0

[nms]

 # Configuración del SNMP

nmsIpAddr = 10.4.1.1

ReadCommunity=public

WriteCommunity=private

AssoDisassoNotify=1

[sntp]

 # Configuración del SNTP

SntpServer = 10.4.1.1

TimeZone = -5

Enable=1

Period=300

[syslog]

SyslogServer=10.4.1.1

Enable=1

Severity=7

[eventlog]

OverWriteAlways=1

AutoFTPLog=1

#***** FIN del Archivo de Configuración FTP para un AP 7220 *********

ANEXO J

CONFIGURACIÓN DEL ROUTER DE BORDE

```
WMN#sh run
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
!
!
interface Ethernet0
 ip address 200.125.200.100 255.255.255.248
 no ip directed-broadcast
 ip nat outside
!
interface Ethernet1
 ip address 10.4.1.10 255.255.255.0 secondary
 ip address 10.8.1.254 255.255.255.0
```

```
 no ip directed-broadcast
 ip nat inside
!
ip nat pool WMN 200.125.200.100 200.125.200.100 prefix-length 29
ip nat pool WMN2 200.125.200.101 200.125.200.101 prefix-length 29
ip nat inside source list 10 pool WMN overload
ip nat inside source list 20 pool WMN2 overload
ip classless
ip route 0.0.0.0 0.0.0.0 200.125.200.97
!
access-list 10 permit 10.8.1.0 0.0.0.255
access-list 20 permit 10.4.1.0 0.0.0.255
!
end
```

ANEXO K

COTIZACIÓN

Quote No:	
Project Name:	**wmesh1**
Created On:	**31 Dic 2009**
Expiration Date:	**15 Ene 2010**
Created with Library:	**9.3.408**
Library Creation Date:	**20 Nov 2007**
All Prices Are In:	**US Dollar**
Price List Used: Nortel - US Dollars(Offline)	

Name	Catalog Num	Vendor	Description	Unit Price	Final Price	Qty	Total Price
Nortel VPN Router 1100, 5 tunnels, single 10/100 Enet	DM1401096	Nortel	Nortel VPN Router 1100, 5 tunnels, single 10/100 Enet, 4-Port Switch, 2 PCI slots, external auto-sensing power supply, Server software w/ (128bit) Encryption, No Power Cord. CPC:N0096142	1.499,00	1.499,00	1	1.499,00
Nortel VPN Router V6.00 S/W 10X0/1100 128 BIT	DM0021020 -6.00	Nortel	Nortel VPN Router V6.00 S/W 10X0/1100 128 BIT CPC:N0036325	Included	Included	1	Included
Contivity Stateful Firewall Lic. - C600/10x0/1100	DM0016009	Nortel	Contivity Stateful Firewall License for the 600/1010/1050/1100 platforms. (Minimum required software for 600: V3.60; Minimum Required Software for 10x0/1100: V4.07. CPC: A0852827	500,00	500,00	1	500,00
Nortel VPN Router Advanced Routing Lic.- 1010/1050/1100	DM0016012	Nortel	Nortel VPN Router Advanced Routing License including OSPF, VRRP, IETF Differentiated Services, and Bandwidth Management for the Contivity 1010/1050/1100. (Minimum required software: V4.07) CPC:A0896771	200,00	200,00	1	200,00
Power Cord 10A/110-120V NA, South Korea	AA0020035	Nortel	Power Cord 10A/110-120V North America, South Korea CPC: N0107237	0,00	0,00	1	0,00
Technical Support Svc Pk C1010/1050/1100	GE5300364	Nortel	Technical Support Services Pack consists of Technical Support Service which features telephone technical support for hardware and the operational software that resides on it plus eService access to all available eService tools. CPC: GE5300364	90,00	90,00	1	90,00
			Nortel VPN Router 1100, 5 tunnels, single 10/100 Enet				**2.289,00**

Wireless AP7215 Indoor	NTE310AG	Nortel	Wireless AP7215 Indoor CPC:N0032800	1.200,00	1.200,00	1	1.200,00
Access Point AP 7220 OmniMount HW Kit	NTE330BA	Nortel	Access Point (AP) 7220 OmniMount HW Kit. CPC: N0002263	80,00	80,00	1	80,00
Wireless AP7215 External Transit Link Antenna Kit	NTE330CG	Nortel	Wireless AP7215 External Transit Link Antenna Kit CPC:N0037553	160,00	160,00	1	160,00
Wireless AP7215 Power Module	NTE330DG	Nortel	Wireless AP7215 Power Module CPC:N0037554	40,00	40,00	1	40,00
Wireless AP7220 Universal Mount HW kit.	NTE330CA	Nortel	Wireless AP7220 Universal Mount HW kit (to be used with Wireless AP7220 NTE300BG and NTE350BG). CPC:N0035820	240,00	240,00	1	240,00
	Wireless AP7215 Indoor						**1.720,00**
Wireless AP7220 with Co-linear Antenna and Base SW (Rel 2) License RTU	NTE350BG	Nortel	Wireless AP7220 with Co-linear Antenna and Base SW (Rel 2) License RTU CPC:N0027921	3.500,00	3.500,00	6	21.000,00
Access Point AP 7220 OmniMount HW Kit	NTE330BA	Nortel	Access Point (AP) 7220 OmniMount HW Kit. CPC: N0002263	80,00	80,00	6	480,00
Wireless AP7215 External Transit Link Antenna Kit	NTE330CG	Nortel	Wireless AP7215 External Transit Link Antenna Kit CPC:N0037553	160,00	160,00	6	960,00
Wireless AP7215 Power Module	NTE330DG	Nortel	Wireless AP7215 Power Module CPC:N0037554	40,00	40,00	6	240,00
Wireless AP7220 5M Ethernet Cable In / Outdoor	NTE330AH	Nortel	Wireless AP7220 5M Ethernet Cable In / Outdoor CPC:N0028819	140,00	140,00	6	840,00
Wireless AP7220 Universal Mount HW kit.	NTE330CA	Nortel	Wireless AP7220 Universal Mount HW kit (to be used with Wireless AP7220 NTE300BG and NTE350BG). CPC:N0035820	240,00	240,00	6	1.440,00
	Wireless AP7220 with Co-linear Antenna and Base SW (Rel 2) License RTU						**24.960,00**
Wireless Gateway 7250 Dual 10/100 Ethernet LAN Ports	NTE352BA	Nortel	Wireless Gateway 7250, Dual 10/100 Ethernet LAN Ports, 1 PCI Exp Slot, (128-Bit) Encryption, (Incl Documentation). No power cord included. CPC: N0033696	7.000,00	7.000,00	1	7.000,00
Power Cord 10A-220/250V North America	AA0020024	Nortel	Power Cord 10A-220/250V North America. CPC: N0107347	0,00	0,00	1	0,00
WLAN 7250 Technical Support Service Pack	GE5300842	Nortel	Technical Support Services Pack consists of Technical Support Service which features telephone technical support for hardware and the operational software that resides on it plus eService access to all available eService tools. CPC: GE5300842	490,00	490,00	1	490,00
	Wireless Gateway 7250 Dual 10/100 Ethernet LAN Ports						**7.490,00**
	TOTAL(US Dollar)						**36.459,00**

ANEXO L

ACRÓNIMOS

802.11	Familia de la IEEE para especificaciones de las redes inalámbricas.
802.11a	Especificación de la IEEE para redes inalámbricas que operan en la banda de frecuencia de 5GHz utilizando modulación OFDM y provee una tasa de transmisión máxima de 54 Mbps.
802.11b	Especificación de la IEEE para redes inalámbricas que operan en la banda de frecuencia 2.4 GHz utilizando modulación CCK y provee una tasa de transmisión máxima de 11 Mbps.
802.11i	Especificación desarrollada por la IEEE para seguridad de las redes inalámbricas LAN.

Access Link	Radio enlace entre un punto de acceso AP 7220 y un usuario móvil terminal.
AL	Enlace de acceso.
ARP	Address Resolution Protocol.
Backbone	El mecanismo primario de conexión en sistema distribuido de manera jerárquica.
Broadcast	Un sistema de entrega de paquetes en el cual una copia de cada paquete es entregada a todos los servidores de red.
CCK	Complementary Code Keying.
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance.
CSMA/CD	Carrier Sense Multiple Access / Collision Detection.
Datagrama	Paquete que contiene información acerca de la dirección destino y los datos.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System. Mecanismo distribuido de nombres/direcciones utilizado en Internet.

EAP	Extensible Authentication Protocol.
EAPOL	Extensible Authentication Protocol Over LAN, un método de encapsulación sobre un mensaje EAP sobre redes LAN.
Flodding	Técnica en la cual la información de la ruta es recibida por un dispositivo de ruteo y es enviada a través de todas las interfaces de ese dispositivo, con excepción de la interface que está recibiendo la información.
Frame	Paquete. Un conjunto de bits que forman un bloque de datos elemental y que es enviado a través de un canal de comunicación.
FTP	File Transfer Protocol.
HA	Home Agent.
HTML	HyperText Transmission Protocol.
ICMP	Internet Control Message Protocol, es un protocolo que identifica los errores y envía mensajes de control a la capa IP.
IP	Protocolo Internet.

IPSec	Seguridad del Protocolo Internet.
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos.
ISP	Proveedor del Servicio de Internet.
LAN	Red de Area Local.
LDAP	Lightweight Directory Access Protocol.
LOS	Línea de Vista.
MAC address	Dirección Física de 6 bytes de un equipo.
MAC	Media Access Control.
Mbps	Megabits por segundo.
MIP	Filtro IP Móvil.
MN	Nodos móviles (inalámbricos).
MTU	Unidad Máxima de Transmisión.
NAP	Network Access Point, punto de acceso de la red.
NAP-R	Network Access Point Router, enrutador del punto de acceso.
NAT	Network Address Translation.

Nodo	Cualquier dispositivo, conectado a una red que transmite y/o recibe datos.
NOSS	Network Operations Support System o Sistema de Soporte de Operaciones de la Red.
OSI	Open Systems Interconnection. Programa internacional de estandarización para facilitar la comunicación entre equipos.
OSPF	Open Shortest Path First.
PC	Computadora personal.
Ping	Packet internet groper. Utilizado para probar la llegada a los destinos mandándoles una petición de ICMP y esperando por un respuesta.
QoS	Calidad de Servicio.
Radius	Remote Authentication Dial-In User Services.
RF	Radio Frecuencia.
RSNA	Robust Security Network Association.
SNMP	Simple / Secure Network Management Protocol.

SNTP	Simple Network Time Protocol.
TL	Enlace de Tránsito.
Transit Link	Radio Enlace entre dos puntos de acceso AP 7220.
VPN	Virtual Private Network, Red Privada Virtual.
WAN	Wide Area Network.
Wi-Fi	“Wireless Fidelity” Alliance compatible 802.11.
WLAN	Wireless LAN, Red de Area Local Inalámbrica.
WPA	Wi-Fi Protected Access, Protocolo de Protección de Acceso al WiFi.

BIBLIOGRAFÍA

1. Molina Enrique, Mompó Vicente, Redes Inalámbricas: IEEE 802.11, www.canal-ayuda.org/a-informatica/inalambrica.htm, consulta Julio 2009.

2. Flores Pérez Carlos, Mecanismos de Enrutamiento para Redes Inalámbricas de Área Local (Wlan) de Tipo Malla, www.conacyt.mx/Centros/Anuarios/.../ANUARIO-2007_CICESE.pdf, 2007, consulta Julio 2009 .

3. Acuña Martínez Diana, Redes Inalámbricas Enmalladas Metropolitanas, Universidad Tecnológica de Bolívar, www.tutorialesenlared.com/manual9722.html, 2007, consulta Julio 2009.

4. Kideok Cho, Wireless Mesh Network: Generation, Products, Testbeds, http://mmlab.snu.ac.kr/courses/2007_advanced_internet/handout/20071015_kdcho.pdf, 2007, consulta Julio 2009.

5. I. F. Akyildiz, Cross Layer Design In Wireless Mesh Networks, Georgia Institute of Technology, http://www.cttc.cat/resources/doc/080704-akyildiz-xlayer-wmn-080702-20333.pdf, consulta Julio 2009 .

6. Acuña Martínez Diana, Redes Inalámbricas Enmalladas Metropolitanas, Universidad Tecnológica de Bolívar, www.tutorialesenlared.com/manual9722.html, 2007, Pág. 70, consulta Agosto 2009.

7. Blanco Oscar, Evaluación de una red de sensores con protocolo AODV y tecnología radio IEEE 802.15, upcommons.upc.edu/pfc/bitstream/2099.1/3723/2/41791-2.pdf, 2005, Pág. 23, consulta Agosto 2009.

8. *Hong X., Scalable Routing Protocols for Mobile Ad Hoc Networks,* www.cs.ucla.edu/NRL/wireless/uploads/ntwkmgz02-hxy.pdf, consulta Agosto 2009.

9. Xue Yuyan, Security Issues in Wireless Mesh Networks, cse.unl.edu/~yxue/SWMN.ppt, 2007, Septiembre 2009.

10. Wang Xiao-dong, Zhao Fuyong, A Method and System for Distributed Roaming Services for Mobile Users in Wireless Mesh Networks, http://www.wipo.int/pctdb/en/wo.jsp?IA=US2005042557&DISPLAY=DESC, 2005, consulta Septiembre 2009.

11. Tropos, equipos de la solución Wireless Mesh, http://www.tropos.com, consulta Octubre 2009.

12. BelAir Networks, equipos de la solución Wireless Mesh, http://www.belairnetworks.com, consulta Octubre 2009.

13. SkyPilot Networks, equipos de la solución Wireless Mesh, http://www.skypilot.com, consulta Octubre 2009.

14. Firetide, equipos de la solución Wireless Mesh, http://www.firetide.com, consulta Octubre 2009.

15. Cisco Networks, equipos de la solución Wireless Mesh, www.cisco.com, consulta Octubre 2009.

16. Motorola, equipos de la solución Wireless Mesh, www.motorola.com, consulta Octubre 2009.

17. Nortel, equipos de la solución Wireless Mesh, www.nortel.com/solutions/wrlsmesh/collateral/nn106481.pdf, consulta Octubre 2009.

18. Nortel, Wireless Mesh Network Basics, Part No: NN47255-100, 2007, Pág. 36.

19. Nortel, Planning and Engineering a Nortel Wireless Mesh Network, Part No: NN47255-100, 2005, Pág. 36.

20. Paredes Vicente, Extendiendo el Alcance de VoIP con las Redes Wireless Mesh, Gruein – Nortel, 2008.

21. Robson Julius, AP7220 Link Budget Parameters for RF Range Prediction, Nortel, 2005.

22. Ian F. Akyildiz, Xudong Wang, Weilin Wang, Wireless mesh networks: a survey. Computer Networks, pag. 445–487, 2005.

23. Yang Zhang, Jijun Luo, Honglin Hu, Wireless mesh networking: “Architectures, Protocols and Standards”, Auerbach Publications Taylor and Francis Group, 2006.

24. Gupta P., Kumar P.R., The Capacity of Wireless Networks, IEEE Transactions on Information Theory, Vol. 46, No. 2, 2000,

25. Jason Ernst, Wireless Mesh Networks: Fair Scheduling & Load Balancing, University of Guelph, 2008.

26. Popi Cristian, Festor Olivier, State of the art in Wireless Mesh Networks Management, Madynes Project, 2007.

27. Seignette Marc, Wireless Mesh Networking, www.cisco.com/web/PT/assets/docs/wireless_mesh.pdf*, 2008*

28. Vinagre Díaz Juan, Teoría del Encaminamiento en Redes Ad Hoc Inalámbricas, Universidad Carlos III de Madrid, 2007.

29. Villavicencio Omar, Wireless Mesh Networks: Performance Analysis and Enhancement, University of Puerto Rico, 2008.

30. Pascual Alejandro, Perez Miguel, Diseño e implantación de una red Wi-Fi mesh en un entorno campus, Universidad de Deusto, 2007.

31. Song Chong, Wireless Mesh Network, KAIST, 2006.