ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN

TELECOMUNICACIONES Y REDES

"ESTUDIO DEL ESTÁNDAR IEEE 802.11S CASO PRÁCTICO: DISEÑO E IMPLEMENTACIÓN DE UNA RED MALLADA PROTOTIPO PARA LA EMPRESA FASTNET CIA LTDA"

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

GLADYS DEL ROCÍO PEÑA BARRENO

RIOBAMBA – ECUADOR

2010

Agradecimiento

A mis padres, Mario y Rosalía. Ejemplo siempre firme de dedicación, comprensión, constancia, cariño y apoyo. Y por darme la oportunidad de contar con una profesión.

A mi madre por su apoyo incondicional, por su amor interminable y por su ejemplo de valor ante momentos difíciles.

A mi esposo por su apoyo y paciencia gracias por esperarme.

A todas las personas que quiero y llevo en mi corazón gracias, ahora se que culmino una etapa más en mi vida, pero empiezo otra.

Dedicatoria

A Dios a mis padres por quienes gracias a su esfuerzo hoy veo culminada una etapa de mi vida y sin su aliento en aquellos momentos duros, lograrlo hubiese sido difícil. Gracias papi y mami, los quiero mucho y siempre los llevo en mi corazón, este triunfo es también por ustedes.

A mi más gran tesoro que es la luz de mi vida gracias por cada día brindarme tu sonrisa y llenarme de fuerzas para continuar, esto es para ti mi gordita

Y a ti vida mia por siempre brindarme tu apoyo y llenarme día a día de una inmensa alegría que ilumina mi vida y llena de amor mi corazón

Rocio

Firmas de Responsabilidad

NOMBRE	FIRMA	FECHA
ING. IVÁN MENES **DECANO DE LA FACULTAD DE** **INFORMÁTICA Y ELECTRÓNICA**	_____	_____
ING. JOSÉ GUERRA **DIRECTOR DE LA ESCUELA** **DE INGENIERÍA ELECTRÓNICA**	_____	_____
ING. DANIEL HARO **DIRECTOR DE TESIS**	_____	_____
ING. WILLIAM CALVOPIÑA **MIEMBRO DEL TRIBUNAL**	_____	_____
LIC. CARLOS RODRÍGUEZ **DIRECTOR DEL DPTO** **DOCUMENTACIÓN**	_____	_____
NOTA DE LA TESIS	_____	

Firma de Autoría

Yo, GLADYS DEL ROCÍO PEÑA BARRENO soy responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

_____

GLADYS DEL ROCÍO PEÑA BARRENO

INDICE DE ABREVIATURAS

AAA Authetication, Authorization and Accounting: Autenticación, Autorización y Administración.

AH Authentication Header: Autentificación De Cabecera.

AODV Ad hoc On Demand Distance Vector: Vector distancia en demanda Ad Hoc

AP Access Point: Punto de Acceso

ACK Acknowledgement: Acuse de recibido.

CSMA/CD Carrier Sense Multiple Access with Collision Detection: Acceso Múltiple con Escucha de Portadora y Detección de Colisiones

CTS Clear To Send: Libre para envío.

DFS Distributed File System: Sistema de archivos distribuidos

DHCP Dinamic host configuration protocol**:** Protocolo de configuración de servidor dinámico

DNS Domain Name System: sistema de nombres de dominio

DSL digital subscriber line: Línea de suscripción digital

EAP Extensible Authentication Protocol: protocolo extensible de autentificación.

ESP Encapsulation Security Payload : cabecera de seguridad encapsulada.

FIFO First In, First Out: primero en llegar, primero en ser servido.

GPSR Greedy Perimeter Stateless Routing: protocolo apátrida del encaminamiento del perímetro codicioso.

IKEv2 Internet key Exchange.

IPsec Internet Protocol Security: seguridad para protoloco Internet.

MN Mesh nodes: nodos mesh.

MPR Multiple protocol router: Enrutador de protocolo múltiple

MS Movil Station: estacion movil

MSK master sesion key: sesión maestra de llaveo.

OFDMA Orthogonal Frequency Division Multiple Access: Acceso multiple de frecuencia ortogonal

OLSR Optimized Link State Routing protocol: Protocolo de encaminamiento de estado de acoplamiento

QoS Quality of Service: Calidad de servicio

RTS Request To Send: Solicitud de envío

UDP Protocol datagram users: Protocolo de datagramas para usuarios

VPN Virtual Private Network: Red privada virtual

WDS Wireless Distribution System: Sistema de distribución inalámbrica

WMN Wireless mesh network: Redes enmalladas inalambricas

WLAN Wireless local area network: Redes inalambricas de area local.

WPA Wi-Fi Protected Access: Acceso de Proteccion Inalambrica.

PSK preshared key: clave precompartida.

SSL Secure Socket Layer: capa de seguridad de zocalo.

TLS Transport Layer Security: Seguridad de la capa de transporte.

INDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

802.11s es el estándar en desarrollo del IEEE para redes Wi-Fi malladas, también conocidas como redes *Mesh*. La malla es una topología de red en la que cada nodo está conectado a uno o más nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

En los últimos años han surgido numerosos proyectos de implantación de redes Wi-Fi malladas. El nicho en el que esta tecnología parece haberse desarrollado de forma más espectacular es el de la redes Wi-Fi municipales, promovidas y financiadas por ayuntamientos. Inicialmente estos sistemas se concibieron como una forma económica de

satisfacer las necesidades de comunicaciones de los ayuntamientos y de los servicios de emergencia, pero últimamente la utilización de Wi-Fi se está planteando como una alternativa gratuita o de bajo coste para proporcionar servicios de banda ancha.

Para mejorar el rendimiento de redes WLAN de malla, algunos nuevos protocolos de comunicación se han desarrollado en los últimos años. Sin embargo, estas soluciones son generalmente de propiedad y con esto evitan que la malla de las redes WLAN tengan interfuncionamiento entre sí. Por este motivo, una norma se convierte en indispensable para redes WLAN mesh. Para satisfacer esta necesidad, un grupo de trabajo IEEE 802.11s, es la especificación de un estándar para red LAN mesh.

JUSTIFICACIÓN

Con el fin de entender el rendimiento y las nuevas funciones que añade el estándar 802.11s en este trabajo se realizará un estudio detallado sobre la norma 802.11s, en el cual se mencionará los diferentes avances que ha tenido el estándar durante estos años los diferentes proyectos realizados en base a IEEE 802.11s.

Este proyecto trata de dotar a ordenadores personales la capacidad de trabajar como APs de una red inalámbricas. Estos APs trabajan utilizando tarjetas inalámbricas PCMCIA. Cada ordenador cuenta con dos tarjetas, una se utilizará en modo Ad-hoc para la comunicación entre los distintos APs y la retransmisión de la información que se transmita por la red. La

otra interfaz trabaja en modo infraestructura, y es la encargada de dar cobertura a los clientes

Las principales razones para la elaboración de este trabajo se fundamentan en el deseo de realizar una aplicación tecnológica sobre un tipo de estructura nueva en el país: la topología de malla. Esta motivación considera, además, fines concretos, como el responder a los requerimientos de la empresa Fastnet Cia. Ltda, que es una empresa de Telecomunicaciones y Proveedor de Servicios Internet (ISP) para empresas, instituciones, cybers, hogares, etc. Con presencia y cobertura a nivel Nacional, la cual desea incorporar en sus servicios tecnología de punta que beneficie a todos los usuarios y que permita acercar las telecomunicaciones a sectores sociales de n es recursos.

OBJETIVOS

OBJETIVO GENERAL

Estudiar el estándar IEEE 802.11s e implementar un prototipo wifi mesh para la empresa Fastnet Cia Ltda

OBJETIVOS ESPECÍFICOS

- Establecer un prototipo mediante software libre que permita conocer y analizar el nuevo estándar 802.11s

- Análisis de las funcionalidades del estándar 802.11s
- Recomendar a la empresa Fast Ethernet la factibilidad de usar este estándar en su empresa

HIPÓTESIS

El estudio del estándar IEEE 802.11s permitirá implementar una red wifi mesh que atienda las necesidades de la empresa Fastnet Cia Ltda

CAPITULO I

MARCO TEÓRICO-CONCEPTUAL

1.1.- Estándar IEEE 802.11

En este capítulo se da una idea de estándar IEEE 802.11, se describe el panorama de la familia IEEE 802.11 y el diseño de la arquitectura de red en malla inalámbrica (802.11s) basado en el actual proyecto de norma.

1.1.1.- Resumen de la familia IEEE 802.11

El estándar **IEEE 802.11** define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana. Aquí se detalla cada uno de los protocolos que existen:

802.11 legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por

señales infrarrojas (IR). IR sigue siendo parte del estándar, si bien no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

Tabla I.I Características de los estándares 802.11

ESTANDAR	CARACTERÍSTICAS
802.11a	Trabaja en la frecuencia de los 5 Ghz con una velocidad de 54Mbits No puede trabajar con equipos 802.11b y tiene menor distancia de cobertura
802.11b	Trabaja en la frecuencia de los 2.4 Ghz con una velocidad de 11 Mbits/s. Introduce CCK (complementary code keying) para llegar a velocidades de 5,5 y 11 Mbps
802.11c	Define características de puntos de acceso como puentes
802.11d	Pensado para permitir el uso internacional de las redes 802.11 locales permite el intercambio de información en los rangos de frecuencia según lo permite en el país de origen del dispositivo
802.11e	Proporciona QoS
802.11f	Es una recomendación para los proveedores de puntos de acceso q permite q los productos sean mas compatibles
802.11g	Trabaja en la frecuencia de los 2,4 Ghz con una velocidad de 54Mbit/sEs compatible con el estándar b y utiliza las mismas frecuencias
802.11h	Trabaja en la frecuencia de los 5 Ghz Intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radar y/o satélite
802.11i	Esta dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación

802.11j	Es equivalente al 802.11h, en la regulación japonesa
802.11k	Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN
802.11n	Trabaja en la frecuencia de los 2,4 Ghz (b y g) y 5 Ghz (a) a una velocidad de 600 Mbps Permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas
802.11p	Trabaja a una frecuencia de 5.9 Ghz Comunicaciones dedicadas ade corto alcance(vehiculos)
802.11r	Permite a la red q establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él
802.11s	Son redes q mesclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la infraestructura
802.11v	Permitirá una getión de las estaciones de forma centralizada(similar a una red celular) o distribuida, a través de un mecanismo de capa 2
802.11w	Permite aumentar la seguridad de los protocolos de autenticación
802.11y	Trabaja a una frecuencia de 3650ª 3700 Mhz Permite q las estaciones registradas operen a una potencia mucho mayor q las tradicionales bandas ISM (hasta 20W PIRE)

1.2.- INFRAESTRUCTURA DE LA WMN

1.2.1.- TOPOLOGIAS DE REDES INALAMBRICAS

Es importante identificar las diferencias entre la topología y el modo de funcionamiento de los dispositivos inalámbricos. La topología se refiere a la disposición lógica de los dispositivos, mientras que el modo de funcionamiento hace referencia al modo de actuación de cada dispositivo dentro de la topología escogida. Las redes Mesh WLAN fueron principalmente construidas para casas, comercio, barrios, comunidades, municipios, seguridad pública, grandes empresas y redes militares. Cada uno de estos mercados representa uno o una combinación de dos importantes topologías Ad Hoc e infraestructura.

1.2.1.1.- Topología Ad-hoc

Una red ad hoc es una red de área local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras, esto quiere decir que Dicha red está formada sin la ayuda de ninguna entidad externa ni servidor central. La configuración de una red de área local inalámbrica en modo ad hoc, se utiliza para establecer una red donde no existe la infraestructura inalámbrica o donde no se requieran servicios avanzados de valor agregado, como por ejemplo una exposición comercial o colaboración eventual por parte de colegas en una localización remota.

Cada nodo no sólo opera como un fin de sistema, también como un router para retransmitir los paquetes. Los nodos son libres moverse y se organizan ellos mismos en una red. Las redes móviles ad hoc no requieren una infraestructura fija tales como estaciones base, además, es una opción atractiva para tener una red de dispositivos móviles de forma rápida y espontánea. Las redes ad-hoc móviles tienen varias características sobresalientes, como son, las topologías dinámicas, la capacidad reducida de ancho de banda, capacidad variable en las ligas, debido a estas características, las redes móviles ad hoc son particularmente vulnerables a ataques por negación de servicio lanzado por un nodo intruso.

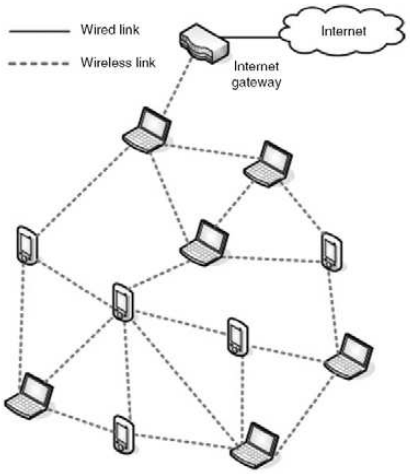

Fig ura I. 1. Topología Ad-hoc (client mesh)

Las redes ad hoc presentan cambios de topología frecuentes e impredecibles debido a la movilidad de sus estaciones. Estas características impiden la utilización de protocolos de encaminamiento desarrollados para redes cableadas y crean nuevos retos de investigación que permitan ofrecer soluciones de encaminamiento eficientes que superen problemas tales como topología dinámica, recursos de ancho de banda y energéticos limitados.

1.2.1.2.- Topología de infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber

varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

Un portátil o dispositivo inteligente, que se caracteriza como una "estación" en términos inalámbricos de una red, primero tiene que identificar los puntos y las redes disponibles de acceso (Ver Figura. I.2). Esto se hace a través del monitoreo de cuadros periódicos desde puntos de acceso, anunciándose así mismo o probando activamente una red en particular utilizando cuadros de prueba. La estación elige una red de las que están disponibles y sigue a través de un proceso de autenticación con el punto de acceso. Una vez que se han verificado entre sí el punto de acceso y la estación, se inicia el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y capacidades. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso en la red para dispersar conocimiento de la ubicación actual de la estación en la red. Sólo después de terminar la asociación la estación puede transmitir o recibir tramas en la red. En la modalidad de infraestructura, todo el tráfico en red de las estaciones inalámbricas en la red pasa a través de un punto de acceso para llegar a su destino y una red LAN ya sea cableada o inalámbrica.

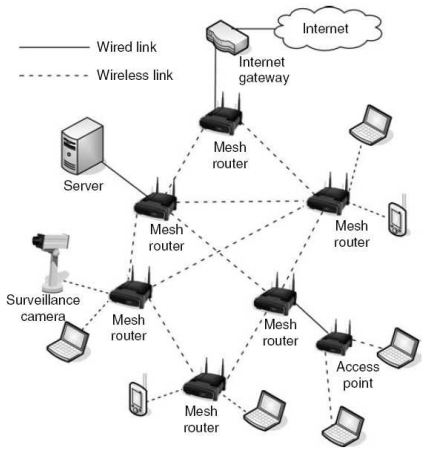

Figura I.2. Topología de infraestructura

1.2.1.3.- Topología hibrida

Esta topología combina la flexibilidad de Ad Hoc y la robustez de la infraestructura. Un WMN híbrido consiste de routers mesh que conforman la espina dorsal de la red. Además, los clientes móviles pueden participar activamente en la creación del enmallado proporcionando funcionalidades de red, tales como encaminamiento y forwarding de paquetes de los datos. Los clientes que ponen estas funcionalidades en ejecución pueden por lo tanto actuar como extensión automática a la pieza más estática de la infraestructura del enmallado. Las redes mesh son muy flexibles y permiten combinar las ventajas de las arquitecturas infraestructura y del cliente y En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida.

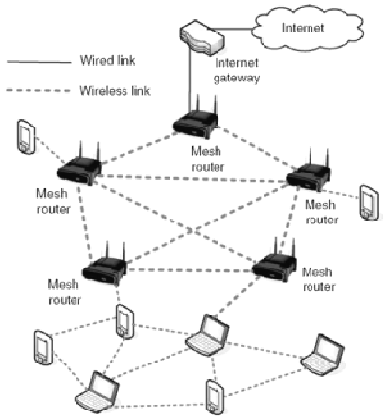

Figura I. 3. Topología Hibrida

1.2.2.- Comparación entre redes Mesh y Ad-hoc

La principal diferencia entre estas redes es la movilidad de los nodos y la topología de red. La red AD HOC tiene una alta movilidad donde la topología de red cambia dinámicamente. Por otro lado están las redes mesh las cuales son relativamente estáticas con su nodos fijos retransmitiendo. Por lo tanto, la movilidad de la red de WMNs es muy baja en comparación con redes AD HOC.

Respecto al funcionamiento del encaminamiento, las redes AD HOC son totalmente distribuidas mientras que en las redes MESH pueden ser total o parcialmente distribuido. Otra diferencia importante entre estas dos categorías de redes es el uso del panorama. Por lo general las redes ad hoc son tenidas en cuenta para usos militares, mientras que las WMNs se utilizan para ambos, usos militares y civiles. Algunos de los usos civiles populares de WMNs incluyen el aprovisionamiento de los servicios baratos del Internet a alamedas de compras, calles, y ciudades. En esta topología no se requiere movilidad de puntos Backhaul exceptuando el roaming de APs de RF o de otro tipo de puntos que cumplan con estas

características. Las casas, comunidades, municipios y los negocios de pequeño y gran tamaño son un ejemplo de redes en infraestructura.

Sin embargo una red IP basada en una subred inalámbrica ad-hoc, también denominada a veces red mesh, está constituida por nodos de funcionalidad idéntica desde el punto de vista de la red, que se comunican entre sí a través de sus radios. No existe una infraestructura jerarquizada, de forma que cada nodo se coordina con los demás como un igual a nivel de enlace y control de acceso al medio. Todos los nodos tienen funcionalidad completa de encaminadores IP y las comunicaciones extremo a extremo suceden por varios saltos (multihop), para lo cual se emplean habitualmente protocolos de encaminamiento dinámico especialmente diseñados para este tipo de redes.

1.3.- ESTANDARIZACIÓN DE LAS REDES MESH 802.11S

Algunas aplicaciones comerciales son interesantes para redes de alta velocidad basadas en redes Mesh de área local se han desarrollado recientemente. Esta tecnología viable económicamente hablando ya que ha sido construida para redes de banda ancha, municipales, de seguridad publica y a gran escala en las llamadas zonas calientes. La arquitectura de las redes Mesh surgió de las redes móviles MANETs usadas para redes militares. El grupo de trabajo IEFT MANET ha estado desarrollando varios protocolos por casi una década. Debido a la popularidad de las redes Mesh y a la cantidad de vendedores que comenzaron a construir dispositivos para redes Mesh se vio la necesidad de crear un estándar que se evidencio en el 2003. El trabajo del grupo de la IEEE que creo el estándar 802.15.5, fue seguido por otro grupo que creo el estándar 802.11s en el 2004. El estándar

IEEE 802.11 especifica las operaciones de acceso a las redes entre clientes y Access points (APs). El estándar 802.11 fue creado para Mesh, Backhaul (infraestructura WLAN) y gateway (infraestructura WLAN a redes LAN cableadas) ver figura I. 4.

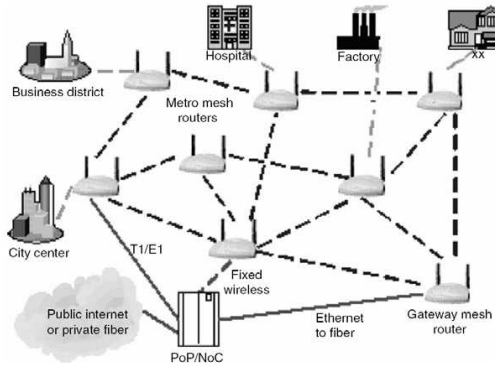

Figura I. 4. Wireless LAN Mesh Networks.

El estándar ofrece flexibilidad, requerida para satisfacer los requerimientos de ambientes residenciales, de oficina, champús, seguridad pública y aplicaciones militares. La propuesta se enfoca sobre múltiples dimensiones: La subcapa MAC, enrutamiento, seguridad y la de interconexión. Además, define sólo sistemas para ambientes en interiores, pero los principales fabricantes de equipos inalámbricos le están apostando también a sistemas en ambientes exteriores.

El estándar IEEE 802.11 esta soportada por dos modos adicionales de operación, el Ad Hoc que puede comunicarse directamente sin necesidad de usar AP y por el modo de distribución inalámbrica que utiliza AP punto a punto, donde cada AP actúa no solo como estación base sino que son nodos despachadores. Sin embargo el estándar 802.11 puede ser usado para formar redes Mesh Efectivas, algunos funcionamientos, seguridad y manejo de problemas que necesitan ser ubicados.

1.3.1.- Redes Wlan tradicionales y Redes Mesh

Una red WLAN tradicional consta de uno o más puntos de acceso (PA) inalámbrico (Access Point) que se conectan mediante un cable UTP categoría 5 directamente a un switch/hub Ethernet hacia la red cableada. De esta misma manera se podrían conectar más puntos de acceso para incrementar el área de cobertura de la red. Con las redes Wi-Fi en malla es posible que estos puntos de acceso se puedan conectar y comunicar entre ellos de forma inalámbrica, utilizando las mismas frecuencias del espectro disperso, ya sea en 2.4 GHz o en la banda de 5.8 GHz. Las redes Wi-Fi en malla son menos ambiciosas pero más reales. Para operar sólo necesitan de clientes ordinarios IEEE 802.11 Las redes Wi-Fi en malla son simples, todos los puntos de acceso comparten los mismos canales de frecuencia. Esto hace a los AP relativamente baratos. El único problema es que el canal es compartido, es decir el ancho de banda de la red. Los APs actúan como hubs, así la malla funciona de manera similar a una red plana construida completamente de hubs; es decir todos los clientes contienden para acceder al mismo ancho de banda.

Los sistemas multiradio utilizan un canal para enlaces hacia los clientes Wi-Fi y el resto para enlaces en malla hacia otros APs. En la mayoría de las arquitecturas los enlaces a los clientes están basados en 802.11b/g, debido a que la banda de frecuencia de 2.4 GHz es la más utilizada por el hardware de los equipos Wi-Fi. En cambio la red de malla está basada en el estándar 802.11a debido a que la banda de 5 GHz está menos congestionada, habiendo menos riesgo de interferencia entre los enlaces de la malla y los clientes. Sin embargo, el estándar 802.11 no soporta nativamente las mallas, así que cada fabricante necesita implementar su propia tecnología propietaria por encima del 802.11a. El estándar 802.11s,

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

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

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

1.3.2.- Mejoras y funcionalidades específicas

Según la normativa 802.11 actual, una infraestructura Wi-Fi compleja se interconecta usando LANs fijas de tipo Ethernet. 802.11s pretende responder a la fuerte demanda de infraestructuras WLAN móviles con un protocolo para la autoconfiguración de rutas entre puntos de acceso mediante topologías multisalto. Dicha topología constituirá un WDS (*Wireless Distribution System*) que deberá soportar tráfico *unicast*, *multicast* y de *broadcast*. Para ello se realizarán modificaciones en las capas PHY y MAC de 802.11 y se sustituirá la especificación BSS (*Basic Service Set*) actual por una más compleja conocida como ESS (*Extended Service Set*). Aún no se conoce mucho de los detalles técnicos del estándar, pero parece que la redacción del mismo se está orientando de forma preferente a dotar a la multitud de puntos de acceso aislados existentes en viviendas y oficinas de la capacidad de conectarse con nodos exteriores pertenecientes a una red Mesh metropolitana existente. De esta forma el grupo de trabajo evitará que sus desarrollos se solapen con las avanzadas tecnologías desarrolladas desde hace años por los fabricantes comerciales de redes Mesh metropolitanas, pero podrá hacer uso de las mismas para ofrecer al usuario final una plataforma estable desde la que acceder a nuevas aplicaciones y servicios. Otra ventaja añadida consiste en que se mejorará la ocupación del espectro radioeléctrico urbano al conectarse el cliente a su propio AP, y no directamente al nodo exterior. Por último, se pondrá especial énfasis en que 802.11s recoja las mejoras en cuanto a tasa binaria, calidad de servicio y seguridad que se incorporen en 802.11n, 802.11e y 802.11i, respectivamente.

Primeras redes mesh

Los estándares 802.11a y 802.11g han incrementado sustancialmente la rata de datos de las WLAN usando esquemas de modulación eficientes (a 54Mbps). EL estándar 802.11 AP (Conocido como punto Mesh [MP] cuando es usado en redes Mesh WLAN). Los puntos MP-a-MP forman una troncal inalámbrica conocida como Mesh Backhaul, la cual proporciona a los usuarios bajo costo, alto ancho de banda y servicios de interconexión multihop con un número de puntos de Internet y con otros usuarios sin la red. Estos dispositivos son llamados Mesh Access Point (MAPs). La figura 4 muestra una red mesh WLAN típica con sus componentes. Una WLAN Mesh esta definida como: Una red Mesh WLAN esta basada en el sistema de distribución inalámbrico del estándar 802.11 (WDS), en la cual una parte DS que consiste en una distribución de dos o mas MPs interconectadas por los puntos 802.11 y la comunicación a través de los servicios Mesh WLAN.

Selección del canal Backhaul

La topología de una red Mesh WLAN pueden incluir MPs con uno o más interfaces de radios y puede utilizar uno o más canales para la comunicación entre MPs. Cuando cada canal esta siendo usado cada interfase de radio opera en una MPs sobre un canal al tiempo. Pero el canal debe cambiar durante el tiempo de vida de la red Mesh de acuerdo a los requerimientos de selección de frecuencias dinámicas (DFS). La selección de un canal específico usado en una red Mesh debe variar de acuerdo a los requerimientos de la aplicación y a las diferentes topologías. Una variedad de interfaces de radio MP que están interconectadas a otras por medio de un canal común, son llamados canales gráficos unificados (UCP). El mismo dispositivo puede tener diversos UCGs. La interfase de radio

establece puntos de conexión con los vecinos que activa la identificación de la red y el perfil, y selecciona su canal basado un valor procedente del canal más alto.

Protocolo de unificación de canal simple

Una interfaz lógica de radio que es configurado en modo unificado de canal simple que funciona con técnicas de escaneo pasivo y activo para descubrir los vecinos MPs. Si una MP no puede detectar un vecino MPs, adopta una identificación de acoplamiento a partir de uno de sus perfiles, y selecciona un canal para la operación, así como un valor inicial de la procedencia del canal. El valor inicial procedente del canal se puede ser iniciado al número de microsegundos más un valor al azar.

1.4.- DESCRIPCION DE OPERACION UNA WMN

1.4.1.- Características de una red Mesh

Una red enmallada esta compuesta por una colección de nodos que se comunican entre si, de manera directa, transmitiendo la información de otros nodos hasta su destino final por medio de múltiples saltos no hay necesidad de una unidad centralizada que los controle el modo de operación de conoce como distribuido. En caso de existir una unidad que administre las condiciones de operación de la red se conoce como centralizado.

Una red enmallada es compuesta por una colección de nodos que se comunican entre sí, de manera directa. Si no hay necesidad de una entidad centralizada que los controle el modo de operación se conoce como distribuido, pero puede existir una entidad central que administre las condiciones de operación de la red, en cuyo caso se conoce como

centralizado. En cualquier caso, la comunicación se realiza entre los nodos directamente y cada nodo puede ser al mismo tiempo fuente o destino de los datos o un enrutador de la información de otro nodo. En la Figura 5 se muestra un diagrama de una red de múltiples saltos, donde la información es llevada desde un extremo a otro por diferentes nodos.

Figura I. 5. Diagrama de Red enmallada.

Si los nodos de la red se conectan de manera autónoma, sin configuración previa, se dice que la red opera en modo *ad hoc.* Si los nodos tienen movilidad, entonces se conocen como redes móviles *ad hoc* o MANET (Mobile ad-hoc Network). Su característica principal es que existe un continuo cambio en la topología de la red, con enlaces que aparecen y desaparecen de modo permanente.

Las características más relevantes de las redes enmalladas inalámbricas son las siguientes:

• **Robustez:** La presencia de enlaces redundantes entre los usuarios permite que la red se reconfigure automáticamente ante fallas.

• **Topología dinámica:** Se supone que las redes enmalladas tienen la capacidad de reaccionar ante cambios de la topología de la red. Por lo tanto la topología cambiante es una condición de diseño necesaria.

• **Ancho de banda limitado:** Como el proceso de comunicación exige transportar datos de otros usuarios y la cercanía de unos con otros precisa una coordinación en los tiempos de transmisión, las redes enmalladas cuentan con enlaces que usualmente permanecen en condiciones de congestión.

Existen esfuerzos importantes en el estándar 802.16-2004 para mejorar el acceso al medio y lograr mejores desempeños en la red. Las primeras versiones de redes enmalladas basadas en el estándar 802.11 son bastante ineficientes en el aprovechamiento del espectro.

• **Seguridad:** La información transmitida se encuentra expuesta a la amenaza de viajar a través de un medio compartido. El estándar define una subcapa de seguridad para proteger la información de los usuarios y evitar el acceso de usuarios no autorizados.

• **Canales de comunicación aleatorios:** A diferencia de las redes fijas, las redes inalámbricas cuentan con la incertidumbre propia de los canales de comunicación de radio. La característica cambiante de los mismos hace bastante inciertas las condiciones de comunicación. El estándar define aspectos como la modulación y codificación adaptativas para hacer frente a este problema.

• **Carencia de modelos de dimensionamiento apropiados:** El modelo de capacidad de redes de datos está orientado a determinar la capacidad del enlace ante procesos de multiplexación de la información de los usuarios. El modelo de capacidad de las redes enmalladas de múltiples saltos es un problema abierto, Las redes enmalladas proveen, sin embargo, condiciones que permiten el acceso a usuarios en regiones apartadas.

Tabla I.1.- Características de las redes inalámbricas enmalladas según la movilidad de los nodos

	Estática	Baja Movilidad	Alta Movilidad
Descubrimiento de la red	Pasivo/Activo	Pasivo/Activo	Activo
Enrutamiento	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones poco frecuentes. Rendimiento altamente estable	Actualizaciones frecuentes. Bajo overhead.
Seguridad	Infrecuentes re-autenticaciones	Infrecuentes re-autenticaciones	frecuentes autenticaciones
QoS	Mecanismos estáticos/lentos.	Mecanismos lentos.	Mecanismos dinámicos/Rápidos
Consumo de energía	Principalmente dispositivos conectados a la red eléctrica.	Una mezcla pero dominan los dispositivos conectados a la red eléctrica.	Principalmente dispositivos basados en el uso de baterías.

1.4.2.- Operación de una red Mesh

La operatividad del sistema no solo depende del buen diseño, sino también de la elección correcta del equipamiento y la robustez de los mismos. Por ello, es necesario diseñar un conjunto de estaciones tanto Gateway como Relay a fin de crear alternativas de diseño según sean los requerimientos. Aparte de estos prediseños, se tienen que tener en cuenta las ganancias de las antenas, direccionalidad de antenas, potencia de amplificadores, etc.

Para crear una red mesh se debe conectar un punto de acceso mesh a algún Tipo de acceso a Internet. Este acceso a Internet puede ser una línea dedicada, una ADSL (Línea de Suscriptor Digital Asimétrica), una SDSL (Línea de Suscriptor Digital Simétrica) o en áreas remotas, por medio del satélite. Todo es compatible siempre que use IP (Protocolo de Internet) El tamaño y el tipo de acceso a Internet se decidirá según una variedad de factores:

• Lo que se tenga disponible

• La cantidad de usuarios que se deba atender

• Los requerimientos de ancho de banda de los usuarios

• El costo

Se configura el primer Mesh-AP con un canal inalámbrico, usualmente un canal 802.11b, un SSID. Al Punto de Acceso a la red Mesh se lo refiere como gateway.

También se utilizan nodos que tienen exactamente la misma programación del nodo gateway. La única cosa que decide si los Mesh-AP se muestran como gateway es si han obtenido una dirección IP de un DHCP o son configurados con una dirección IP fija.

El primer nodo repetidor se desplegará dentro del alcance del primer nodo Mesh-AP, simplemente dándole energía, el mismo canal y el mismo SSID del gateway. Cuando se inicie el Mesh-AP se sabrá que no es un nodo repetidor por el hecho de no haber obtenido una dirección IP. Este tratará de descubrir el nodo gateway. Una vez que haya sido establecido un enlace con un nodo gateway, el tráfico de Internet es encaminado desde el cliente, por medio del nodo repetidor y a Internet por medio del gateway.

De esta manera pueden agregarse más nodos al mesh, y, siempre que el nodo mesh agregado esté dentro del radio de alcance de un nodo que sea o bien un gateway o bien otro nodo que pueda alcanzarlo, entonces el tráfico de Internet será encaminado a través del mesh, por medio de la ruta a Internet más eficiente.

CAPITULO II

ARQUITECTURA WMN

2.1.- PROBLEMAS FUNCIONALES EN REDES MESH Y SUS CAUSAS

Capacidad limitada

A pesar de los grandes avances tecnológicos de la capa física, la capacidad sigue siendo limitada en los sistemas inalámbricos de un solo salto. Por otro lado esta el problema de ancho de banda para las redes Mesh inalámbricas ya que al momento de establecerse la conexión todos los nodos operan sobre el mismo canal de radio. Esto resulta de una substancial interferencia entre las transmisiones de nodos adyacentes de la misma ruta como de la ruta de los nodos vecinos, reduciendo la capacidad de la red.

La capacidad para los nodos mesh es limitada para un sistema de un solo canal comparado con un sistema multicanal. En la tabla II.1 se puede observar el rendimiento de una topología string. Se puede observar fácilmente que a medida que aumentan las longitudes

de las rutas el rendimiento cae. En general son muchos los problemas que contribuyen al mal rendimiento como son las características del protocolo MAC, el problema de los nodos expuestos, los impredecibles y altos errores en un canal inalámbrico. Todos estos son los problemas que agravan los sistemas de un solo canal. Por ejemplo en la figura II.1 se muestra que cuando el nodo 1transmite al nodo 2, especialmente cuando el protocolo MAC se basa en CSMA/CA, los nodos 2 y 3 no pueden iniciar otra transmisión. El nodo 2 es prevenido de transmisiones simultáneas, como interfaces inalámbricas. En la mayoría de las WMNS las comunicaciones son half duplex. De esta manera el nodo 2 se abstrae de establecer comunicación con el nodo 3 porque esta estableciendo comunicación con el nodo 1.

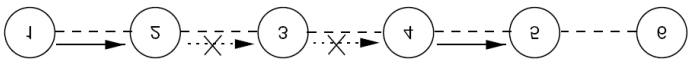

Figura II.6. Un ejemplo de la topología string y problema de nodo expuesto en las WMN

Tabla II.2. Degradación del throughput en las WMN con topología string

	1 Hop	*2 Hops*	*3 Hops*	*4 Hops*	*5 Hops*	*>5 Hops*
Normalized throughput	1	0.47	0.32	0.23	0.15	0.14
$\frac{1}{\text{Hoplength}}$	1	0.5	0.33	0.25	0.2	0.16

La métrica más simple para redes Mesh es la métrica contadora de saltos. Sin embargo el uso de conduce a la selección de trayectoria optima. Un gran problema es que cuando los

saltos son cortos y se vuelven extensos Se presenta un error y se desbalancean las cargas del trafico a través de la red, lo cual reduce la capacidad de la red.

El problema de limitación de capacidad es tocado mas a fondo por el protocolo TCP que no puede utilizar con eficacia la anchura de banda disponible. El protocolo TCP el ACK que es una señal que pide retransmisión de la ruta del paquete que se usa en el caso de que el paquete se pierda en un salto intermedio. Esto conduce al despilfarro de la anchura de banda en todos los saltos precedentes donde las transmisiones necesiten del ACK, pudiéndose utilizar mejor en trasmisiones en las cuales el paquete es transmitido en forma acertada.

Otro problema que limita la capacidad es el control ineficiente de la congestión. El control de la congestión de TCP tiene en cuenta pequeños segmentos de la información del paquete para detectar la congestión de la red. Sin embargo en redes inalámbricas los paquetes también se caen debido a los errores presentes en los pequeños segmentos que calculan la congestión de la red.

El TCP no puede distinguir entre estos pequeños segmentos y la congestión verdadera. Los errores del canal pueden conducir a la falta de aprovechamiento substancial de la red.

Confiabilidad y robustez: Otra motivación importante para usar WMNs es que debe mejorar la confiabilidad y la robustez de la comunicación. La topología parcial del acoplamiento en una WMN proporciona alta confiabilidad y diversidad de la trayectoria contra faltas del nodo y del acoplamiento. Las WMNs proporcionan el ingrediente más importante para la robustez en la comunicación diversidad. Por ejemplo en los sistemas

inalámbricos, el error en los canales son altos en comparación con los sistemas cableados. Sin embargo la alta degradación de la comunicación por los errores en los canales es necesaria. Esto es muy importante cuando las WMNS emplean frecuencias que están por fuera del espectro. De esta manera las WMNS emplean diferentes frecuencias al usar diferentes interfaces multiradio, cuando es difícil alcanzar una sola interfaz de radio.

Manejo de recursos: El manejo de Recurso se refiere al manejo eficiente de los recursos de la red tales como almacenamiento de energía, anchura de banda e interfaces. Por ejemplo, los recursos de energía se pueden utilizar eficientemente en las WMNs con la reserva limitada de la energía si cada nodo en el sistema tiene una nueva interfaz de baja potencia además de una interfaz regular. El consumo de energía total, incluso en modo ocioso, depende mucho del tipo de interfaz. Por lo tanto, la IEEE 802.11 baso las WMNs con la reserva limitada de la energía, un interfaz de baja potencia y de datos bajos de tarifas adicionales se pueden utilizar para llevar la información que está fuera de banda para controlar la alta potencia y los altos datos en la interfaz de los datos. Los recursos de la anchura de banda se pueden también manejar mejor en un ambiente del multiradio. Por ejemplo, si la carga es balanceada a través de interfaces múltiples se podría contribuir a prevenir cualquier canal particular que provoca congestionado pesado y embotellamiento en la red.

PROBLEMAS EN EL DISEÑO DE UNA WMN

Hay muchos problemas que necesitan ser considerados cuando se diseña una WMN para una aplicación en particular. Estos problemas de diseño se pueden clasificar ampliamente en problemas de arquitectura y de protocolos. Una red WMN puede estar diseñada de acuerdo a tres diferentes arquitecturas de red basadas en topologías de red: WMNs planas, WMNs jerárquicas y WMNs hibridas.

WMNs Planas: En una WMN plana, la red esta formada por los dispositivos del cliente que actúan como rebajadoras. Aquí, cada nodo está en el mismo nivel que el de sus pares. Los nodos inalámbricos del cliente coordinan entre sí mismos para proporcionar el encaminamiento, la configuración de red, el aprovisionamiento del servicio, y otros aprovisionamientos de uso. Esta arquitectura es la más cercana a una red inalámbrica ad hoc y es el caso más simple entre las tres arquitecturas de WMN. La ventaja primaria de esta arquitectura es su simplicidad, y sus desventajas incluyen la carencia del escalabilidad de la red y de los altos costos de recursos. Los problemas primarios a la hora de diseñar una WMN plana son el esquema de dirección, el encaminamiento, y el descubrimiento de esquemas de servicio. En una red plana, la dirección es una de los problemas que pueden convertirse en un embotellamiento contra escalabilidad.

WMNs Jerárquicas: En un WMN jerárquico, la red tiene grados múltiples o niveles jerárquicos en los cuales los nodos del cliente de WMN forman están en la parte mas baja de la jerarquía. Estos nodos clientes pueden comunicarse con la red troncal formada por routers de WMN. En la mayoría de los casos, los nodos de WMN son los nodos dedicados que forman una red troncal de WMN. Esto significa que los nodos de la troncal no originar o terminar datos en un tráfico determinado como los nodos del cliente de WMN. Su

responsabilidad es la de organizar y de mantener la red de espina dorsal de proporcionar paquetes a los routers de WMN algunos de las cuales en la red troncal pueden tener interfaces externas al Internet.

WMNs hibridas: Éste es un caso especial de WMNs jerárquico donde el WMN utiliza otras redes inalámbricas para la comunicación. Por ejemplo, el uso de otras WMNs basadas en infraestructura tal como redes celulares, redes de WiMAX, o redes basadas en los satélites. Ejemplos de tales WMNs híbridas incluyen las redes celulares multihop, rendimiento de procesamiento radio realzada en las redes locales del lazo y redes ad hoc de celulares unificadas. Una solución práctica para tal híbrido WMN para los usos de la respuesta de la emergencia es la plataforma de CalMesh. Este es el híbrido WMN que puede utilizar las tecnologías múltiples para WMN y el establecimiento de una red inalámbrica con acoplamiento de transporte del backbone y de la parte posterior. Puesto que el crecimiento de WMNs depende grandemente de la manera como trabaja con otras soluciones inalámbricas existentes de una red, esta arquitectura llega a ser muy importante en el desarrollo de WMNs.

2.2.- CLASIFICACION DE LOS PROTOCOLOS DE RUTEO DE REDES ENMALLADAS

La tarea principal de los protocolos de ruteo es la selección de el camino entre el nodo fuente y el nodo destino. Esto tiene que ser hecha de una manera confiable, rápida, y con gastos indirectos mínimos. En general, los protocolos de ruteo pueden ser clasificados en los basados en topología y en los basados en posición. Los protocolos de ruteo basados en

topología seleccionan trayectorias basadas en información topológica, como por ejemplo los enlaces de nodos. Los protocolos de ruteo basados en posición seleccionan trayectorias basadas en la información geográficas con algoritmos geométricos.

También hay protocolos que combinan esos dos conceptos.

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

Otras posibilidades para la clasificación de protocolos de ruteo son: Flan vs hierarchical, distance vector vs. link state, source routing vs. hopby- hop routing, single-path vs. multipath.

En principio las redes mesh pueden manejar cualquier clase de protocolo de ruteo descrita anteriormente. Sin embargo no cada protocolo trabajará bien. La selección de un protocolo de encaminamiento conveniente depende del panorama, uso, y requisitos de funcionamiento.

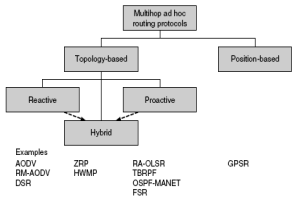

Figura II.7. Clasificación de protocolos de ruteo en WMN

2.2.1.- Protocolos basados topología (Topology based)

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

AODV (Ad Hoc On-Demand Vector Routing)

AODV es un protocolo de ruteo muy popular para MANETs el cual es un protocolo de ruteo reactivo. Este protocolo permite el enrutamiento dinámico, autoarranque y multihop entre todos los nodos móviles que participan en la red. AODV permite a todos los nodos obtener las rutas rápidamente para las nuevas destinaciones y no requiere que los nodos mantengan las rutas hacia los destinos que no están activos en la comunicación.

El protocolo de enrutamiento está diseñado para redes móviles ad hoc con gran cantidad de nodos y con distintos grados de movilidad. Este protocolo se basa en que todos los nodos tienen que confiar en los otros para transportar sus datos, aunque sea por el uso de una clave preconfigurada, o activando mecanismos para evitar la participación de nodos intrusos.

En este apartado lo que se intenta es dar una breve introducción de sus características y sus modos de funcionamiento básicos, así como sus tablas y Mensajes más característicos sin entrar en el formato de estos.Una característica distintiva de este protocolo es el uso del número de secuencia para cada ruta. Este número de secuencia es creado por el destino para ser incluido con la información necesaria para los nodos que requieren la información. El uso de estos números implica que no se crean *bucles* y la facilidad de programación.

Este protocolo define tres tipos de mensajes: Route Requests (RREQs), Route Replies (RREPs) y Route Errors (RERRs). Estos mensajes se reciben vía UDP. Mientras todos los nodos tengan las rutas correctas de cada nodo el protocolo no intercambia mensajes ni tiene ninguna función. Cuando una ruta hacia un nuevo destino es necesaria, el nodo que la necesita envía una mensaje broadcast RREQ que llega al destino, o a un nodo intermedio que tiene una ruta suficientemente “fresca” hacia el destino. Una ruta es “fresca” cuando el número de secuencia hacia el destino es como mínimo tan grande como el número que contiene el RREQ. La ruta se considera disponible por el envió de un mensaje RREP hacia el nodo que originó el RREQ. Los nodos monitorizan el estado de las conexiones de los nodos, a un salto, participantes en las rutas activas. Cuando una conexión se rompe en una ruta activa, se envía un mensaje RERR para notificar a los otros nodos la pérdida de la conexión.

Este protocolo tiene una tabla de rutas. La información de la tabla de rutas debe guardarse incluso para las rutas de corta vida. Los campos que tiene cada entrada de la ruta son los siguientes:

• IP de destino.

• Número de secuencia de destino.

• *Flag* número de secuencia de destino válido.

• Otros estados y *flags* de enrutamiento (válido, invalido, reparable...).

• Interfaz de red.

• Contador de saltos.

• Salto siguiente.

• Listado de precursores.

• Tiempo de vida.

Terminología

En este apartado se definen algunos nombres y sus significados que se utilizan en este protocolo:

• **Ruta activa:** una ruta que tiene una entrada en una tabla y esta marcada como válida. Sólo estas rutas se pueden usar para la retransmisión.

• **Broadcast:** estos paquetes no deben ser transmitidos por la red en exceso, pero son útiles para la transmisión de los mensajes del AODV por la red.

• **Nodo retransmisión:** nodo que permite la retransmisión de paquetes hacia otros nodos, por medio de enviar los paquetes hacia el siguiente salto.

• **Ruta de retrasmisión**: una ruta configurada para enviar paquetes de datos desde el nodo que origina el descubrimiento de la ruta hacia el destino deseado.

• **Ruta inválida:** una ruta que ha expirado, tiene el estado inválido. Estas rutas se utilizan para guardar una ruta válida anterior y de este modo tener la información durante más tiempo. Una ruta inválida no puede ser utilizada para la retransmisión de paquetes.

• **Nodo originario:** un nodo que inicia el mensaje de descubrimiento de ruta para ser procesado y poder ser retransmitido por otros nodos.

• **Ruta contraria:** una ruta configurada para retransmitir el paquete (RREP) desde el destinatario hacia el que ha originado el mensaje.

• **Número de secuencia:** un número incremental que mantiene cada nodo originario. En los mensajes del protocolo AODV se usa por los otros nodos para determinar la “frescura” de la información que tiene el nodo Originador.

Mantenimiento de números de secuencia

Cada entrada de la tabla de cada nodo debe incluir la última información sobre el número de secuencia para la dirección IP del nodo destino. Este número de secuencia se llama “número de secuencia de destino”. Se actualiza cada vez que un nodo recibe nueva información del número de secuencia por los mensajes RREQ, RREP o RERR. Este protocolo depende de que cada nodo de la red mantenga su propio número de secuencia de destino para garantizar que no haya bucles. Un nodo destinatario incrementa su propio número de secuencia en dos circunstancias:

• Inmediatamente antes que un nodo origine el descubrimiento de una ruta, debe incrementar su propio número de secuencia.

• Inmediatamente antes que el nodo destino origine un mensaje RREP como respuesta a un RREQ, este nodo debe actualizar su número de secuencia, eligiendo el valor máximo entre su actual número de secuencia o el número del paquete RREQ que le ha llegado.

Entradas de la tabla de enrutamiento

Cuando un nodo recibe un paquete de control desde un vecino, crea o actualiza una ruta hacia un destino particular o una subred, el nodo comprueba su tabla de enrutamiento por una entrada para el destino. La ruta se actualiza en los siguientes casos:

• El número de secuencia es mayor que el que hay en al tabla de enrutamiento.

• El número de secuencia es igual, pero el nuevo valor del contador de saltos más uno, es menor que el valor que tenia la ruta de la tabla de enrutamiento.

• El número de secuencia es desconocido.

Las entradas de la tabla tiene un campo de tiempo de vida, este tiempo se determina por el paquete de control que llega, o se toma un valor determinado.

Generación de peticiones de rutas

Un nodo envía un mensaje RREQ cuando determina que necesita saber la ruta hacia un destino y no lo tiene en su tabla de enrutamiento o es una entrada no válida. En ese momento se envía un mensaje RREQ con el valor del número de secuencia de destino igual

al último número conocido para este destino. El valor del número de secuencia de origen en el mensaje RREQ es el número de secuencia del nodo que es incrementado antes del envío del mensaje.

Al tener en cuenta que las comunicaciones son bidireccionales, además de la ruta para llegar al destino también es necesario saber una ruta de vuelta. Para este cometido cualquier nodo intermedio que genere un mensaje de respuesta (RREP) debe también realizar una acción que notifique al nodo destino una ruta de vuelta hacia el nodo origen.

Para no crear congestión en la red ni hacer que los mensajes circulen indefinidamente por ella, el nodo que origina peticiones debe indicar un TTL máximo a los mensajes y además seleccionar un *timeout* para esperar una respuesta. Tanto el *timeout* como el TTL son calculados de manera periódica y tiene en cuenta el tamaño de la red y el tiempo que tarda un paquete en cruzarla.

Procesamiento y retransmisión de peticiones de ruta

Cuando un nodo recibe un RREQ, crea o actualiza una ruta hacia el salto anterior. Posteriormente comprueba que no haya recibido una mensaje con el mismo ID y origen y si lo ha recibido descarta este nuevo mensaje. En este apartado se explicará las acciones que se realizan cuando este mensaje no se descarta.

Lo primero que se hace es aumentar el valor del contador de saltos en uno.

Después, el nodo busca una ruta hacia la IP origen del mensaje. Si no existe se debe crear esta nueva ruta de vuelta. Una vez se ha creado esta ruta de vuelta se siguen las siguientes acciones:

• El número de secuencia origen se compara con el número de secuencia hacia el destino que se tiene en la tabla, y si es mayor se copia en ella.

• Se valida el campo de número de secuencia.

• El siguiente salto en la tabla de enrutamiento se convierte el nodo desde donde nos ha llegado el mensaje.

• Se copia el número de saltos en la tabla de enrutamiento.

Generación de respuesta de ruta

Un nodo genera un mensaje RREP si él mismo es el destino, o tiene una ruta activa hacia el destino y el número de secuencia de la entrada de la tabla es mayor que el del mensaje RREQ. Una vez se genera el RREP el nodo descarta el mensaje RREQ.

Si un nodo no genera un RREP y el valor del TTL es mayor de uno entonces actualiza y envía el mensaje RREQ a una dirección *broadcast*.

Si el nodo que genera el mensaje RREP no es el nodo destino sino que es un nodo intermedio, copia su propio número de secuencia para el destino en el campo de número de secuencia destino del mensaje RREP. Entonces este nodo intermedio actualiza la ruta de retransmisión poniéndose a él como último nodo en la lista de precursores.

Recepción y retransmisión de respuesta de ruta

Cuando un nodo recibe un mensaje RREP busca una ruta hacia el salto anterior, si es necesario se crea esta ruta. Posteriormente el nodo incrementa el contador de saltos en el mensaje. Entonces se crea una ruta para llegar al destino si no existe. De otra manera, el nodo compara el número de secuencia de destino del mensaje con el que tiene guardado. Después de la comparación la ruta existente se actualiza en los siguientes casos:

• El número de secuencia en la tabla de enrutamiento está marcado como inválido.

• El número de secuencia de destino en el mensaje es mayor que el que el nodo tiene guardado y el valor es válido.

• Los números de secuencia son iguales pero la ruta está marcado como inactiva.

• Los números de secuencia son los mismos, y el nuevo valor del contador de saltos es menor.

Cuando se actualiza una entrada en la tabla la ruta se marca como activa, el número de secuencia de destino también se marca como válido y en el siguiente salto en la entrada de la tabla se asigna el nodo del que ha llegado el mensaje RREP. También se debe actualizar el nuevo valor del contador de saltos, el tiempo de expiración de la ruta y el número de secuencia de destino, se debe actualizar por el número de secuencia del mensaje RREP.

Mensajes de error (RERR)

Normalmente una ruta errónea o el corte de un enlace necesitan un procedimiento similar. Primero invalidar las rutas existentes, listar los destinos afectados, determinar los vecinos afectados y enviar un mensaje apropiado RERR a estos vecinos.

Un nodo inicia el procesamiento de un mensaje RERR en tres situaciones:

• Si detecta la caída de un enlace para el siguiente salto de una ruta activa en su tabla de enrutamiento mientras envía datos.

• Si recibe un paquete de datos hacia un nodo del que no tiene ninguna ruta activa.

• Si recibe un mensaje RERR desde un vecino por una o más rutas activas.

Ejemplo 1

En la figura II.8 se puede ver como un nodo (A) busca la ruta hacia otro nodo (J) del que no conoce el camino. Lo primero que hace el nodo A es enviar un mensaje broadcast RREQ hacia todos los nodos, preguntando por el nodo J, con el que se quiere comunicar. Cuando el mensaje RREQ llega al nodo J este genera un mensaje RREP de respuesta. Este mensaje se envía como unicast de vuelta hacia el nodo A utilizando las entradas en memoria de los nodos H, G y D.

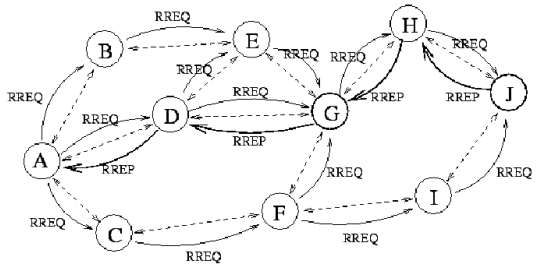

Figura II.8. Ejemplo de búsqueda de un nodo

EJEMPLO 2

Cuando el nodo fuente S quiere enviar paquetes de datos a un nodo destino D pero no tiene una ruta a D en su tabla de ruteo, una ruta de descubrimiento tiene que ser hecha por S. los paquetes de datos son protegidos durante el descubrimiento de la ruta. Ver la figura para una ilustración del proceso de una ruta de descubrimiento. El nodo fuente S difunde una petición de ruta, llamada (RREQ) , a través de la red.

Además de varias FLAGS, un paquete de RREQ contiene el hopcount, un identificador de RREQ, la dirección destino y el número de serie de la numeración, y el de la dirección originaria y de serie originaria.

El campo hopcount contiene la distancia a el autor de el RREQ, el nodo de fuente S. ese va a ser el numero de saltos que el RREQ ha realizado hasta ahora. El RREQ ID combinado con la dirección originaria identifica una solamente una petición de ruta. Esto se utiliza para asegurarse de que los rebroadcasts de un nodo manden una petición de la ruta solamente una vez para evitar confusiones o coaliciones en los datos, aunque un nodo recibe el RREQ varias veces de sus vecinos. Cuando un nodo recibe un paquete RREQ es procesado como sigue acontinuación:

• La ruta del salto anterior de el cual se ha recibido el paquete de RREQ escreado o es actualizado.

• El RREQ ID y la direccion de donde es originada son verificadas para ver si este RREQ ha sido recibido anteriormente. Si es asi, el paquete es desechado.

• El hopcount es aumentado en 1.

La ruta inversa a el nodo fuente, nodo S, es creada o actualizada.

• Si el nodo es el destino solicitado, este nodo genera una respuesta de la ruta (RREP) y envía el paquete RREP de nuevo al nodo origen a lo largo de la ruta inversa creada al nodo S. de la fuente.

• Si el nodo no es el destino pero tiene un camino valido a D, este publica un RREP a la fuente dependiendo solamente de la bandera (flags) del destino.

Si los nodos intermedios contestan a RREQs, puede ser que sea el caso que el destino no detecte cualquier RREQ es decir no llegara, de modo que no tenga una ruta trasera a la fuente. Si las flags gratuita de RREP se fija en el RREQ, el nodo intermedio que contesta enviará un RREP gratuito a el destino. Esto fija la ruta al autor del RREQ destino. Si el nodod no genera una RREP, el RREP es actualizado y regenerado si el TTL es > 1.

En recibo al mensaje de RREP, un nodo creará o pondrá al día su ruta a el destino D. El hopcount es incrementado por uno, y el RREP actualizado será remitido al nodo origen del RREQ correspondiente. Eventualmente, el nodo S de la fuente recibirá un RREP si existe

una ruta al nodo destino. Los paquetes protegidos de los datos se pueden ahora enviar al nodo D en la trayectoria nuevamente descubierta.

La información de la conectividad es proporcionada y mantenida periódicamente difundiendo mensajes de gestión de protocolo ruteo. Si un nodo no ha enviado un mensaje de difusión, un mensaje de RREQ, con el ultimo intervalo HELLO, el nodo puede difundir un HELLO MESSAGE. Un HELLO es realmente un RREP con el TTL= 1 y el mismo nodo como destino.

Si un nodo no recibe ninguna clase de paquetes de un nodo vecino por un tiempo definido, el nodo considera que el enlace con ese nodo vecino se encuentra roto. Cuando ha sucedido una caída en el enlace, el nodo antes de que el enlace haya caído comprueba primero si cualquier ruta activa había utilizado este enlace antes. Si éste no es el caso, nada se puede hacer. Por otra parte, si ha habido trayectorias activas, el nodo puede procurar una reparación local. El nodo envía un RREQ para establecer una nueva segunda mitad de la ruta al destino.

El nodo que realiza la reparación del local protege los paquetes de los datos mientras que espera cualquier contestación de la ruta. Si la reparación local falla o no se ha procurado, el nodo genera un mensaje del error de la ruta (RERR) que Contiene las direcciones y los números de serie correspondientes a el destino de todas los destinatarios activas que lleguen a ser inalcanzable debido a la falta del enlace15. El mensaje de RERR se envía a todos los vecinos que sean precursores de las destinaciones inalcanzables en este nodo. Un nodo que recibe un RERR invalida las entradas correspondientes en su tabla de encaminamiento.

Quita todas las destinaciones de las cuales no tener el transmisor del RERR como salto siguiente de la lista

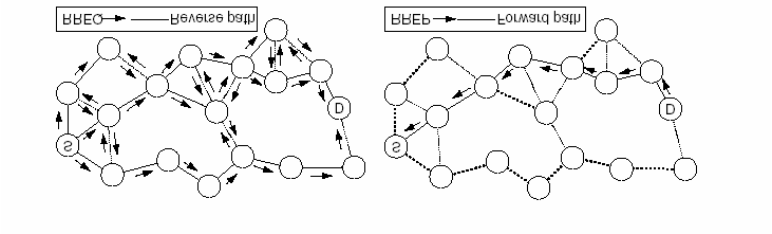

Figura II. 9. Descubrimientos de la ruta AODV a) ruta de petición (izq) y b) ruta de contestación (der).

DSR (Dynamic Source Routing)

El protocolo DSR se fundamenta en el encaminamiento desde el origen, es decir, los paquetes de datos incluyen una cabecera de información acerca de los nodos exactos que deben atravesar. No requiere ningún tipo de mensajes periódicos (reactivo), disminuyendo así la sobrecarga con mensajes de control.Además ofrece la posibilidad de obtener, con la solicitud de una ruta, múltiples caminos posibles hacia el destino. Tampoco son un problema, a diferencia de la mayoría de protocolos de encaminamiento en este tipo de redes, los enlaces unidireccionales. Para poder realizar el encaminamiento en el origen, a cada paquete de datos se le inserta una cabecera DSR de opciones que se colocará entre la cabecera de transporte y la IP. Entre dichas opciones se incluirá la ruta que debe seguir el paquete nodo a nodo. Cada nodo mantiene una memoria caché de rutas en la que se van almacenando las rutas obtenidas a través de procesos de descubrimiento de rutas ya sean propios o obtenidos a través de escuchas en la red. En los procesos de descubrimiento de rutas se generan mensajes de solicitud, respuesta y error siendo estos mensajes ROUTE REQUEST, REPLY y ERROR respectivamente.

OLSR (Optimized Link State Routing Protocol)

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

La selección de los nodos MPR reduce el número de retransmisiones necesarias para enviar un mensaje a todos los nodos de la red. OLSR optimiza la reacción a cambios en la topología reduciendo el intervalo de transmisión de los mensajes periódicos de control. Como este protocolo mantiene rutas hacia todos los destinos de la red trabaja muy bien en redes donde el tráfico es aleatorio y esporádico entre un gran número de nodos.

OLSR trabaja de manera distribuida sin ninguna entidad central. Este protocolo no requiere transmisiones seguras de mensajes de control porque los mensajes son periódicos, y se pueden permitir algunas pérdidas. Tampoco necesita una recepción de mensajes secuencial, se utiliza números de secuencia incrementales para que el receptor sepa que información es más reciente.

Terminología

Palabras claves para entender el funcionamiento de este protocolo:

• **Nodo:** Router que implementa el protocolo OLSR.

• **Interfaz OLSR:** interfaz de un equipo que participa en el protocolo OLSR.

También se debe tener en cuenta que hay otras interfaces en estos equipos que no trabajan en el protocolo.

• **Dirección principal:** la dirección principal de un nodo, se utilizará como la dirección de origen del tráfico de control en OLSR emitida por este nodo.

• **Nodo vecino:** un nodo X es vecino de otro nodo Y, si el nodo Y puede escuchar nodo X. Existe un enlace entre los dos nodos. Dos nodos son vecinos si ambos se encuentran dentro del área de cobertura del otro.

• **Vecino a 2 saltos:** un nodo "escuchado" por un vecino. Nodo, no vecino, que está dentro del área de cobertura de un nodo vecino.

• **Vecino a 2 saltos estricto:** un nodo que es vecino de un vecino del nodo que se esta mirando.

• **MPR (Multiponit relay):** un nodo que es seleccionado por su vecino, nodo X, para retransmitir todos los mensajes *broadcast* que recibe del nodo X.

• **MPR selector (MS):** un nodo que ha seleccionado su vecino como su MPR.

MPS de un nodo x es todo aquel que tiene a x como MPR.

• **Enlace:** pareja de interfaces OLSR sensibles a "escuchar" el otro. Los enlaces pueden ser simétricos (enlace bidireccional), asimétricos (sólo verificados en un sentido).

• **Vecindario simétrico de 1 salto:** de un nodo X es el grupo de nodos que tiene un enlace simétrico hacia X.

OLSR está modulado para tener un núcleo de funcionalidades, que siempre es requerido, y un grupo de funcionalidades auxiliares.

Funcionamiento núcleo

El núcleo especifica el comportamiento de un nodo que tiene interfaces OLSR.

Se basa en las siguientes funcionalidades:

• **Formato de paquete y retransmisión:** OLSR se comunica mediante un formato de paquete unificado para todos los datos del protocolo. El propósito de esto es facilitar la extensión del protocolo. Estos paquetes se envían como datagramas UDP. Cuando recibimos un paquete básico, un nodo examina el mensaje, y basándose en un campo donde se indica el tipo de mensaje determinará el procesamiento del mensaje que seguirá los siguientes pasos:

• Si el paquete no contiene mensaje (el tamaño es demasiado pequeño) se descarta.

• Si el valor del TTL es menor o igual que 0 también se descarta.

• **Condiciones de proceso:** Si es un mensaje es duplicado (la dirección de origen y la número de secuencia ya se han tratado) no se procesa. En caso contrario el paquete es tratado de acuerdo al tipo de mensaje que haya llegado.

• **Condiciones de retransmisión:** Si es un mensaje duplicado no se retransmite, si no es duplicado se retransmite el mensaje siguiendo el algoritmo del tipo de mensaje.

• **Percepción de enlace:** Se consigue saber el estado del enlace mediante el envío de mensajes “HELLO”. El propósito de esta funcionalidad es que cada nodo tenga asociado un estado en el enlace a cada uno de sus vecinos. El estado puede ser simétrico (enlace verificado es bidireccional) y asimétrico indica que los mensajes “HELLO” se han escuchado pero no podemos asegurar que este nodo escuche las respuestas.

• **Detección de vecino:** Dada una red de nodos con sólo una interfaz, un nodo debe deducir los vecinos que tiene mediante la información intercambiada durante la percepción de enlace. Cada nodo debe tener guardados su grupo de vecinos. Cada vecino debe tener asociado el estado del enlace. Cuando se detecta la aparición de un nuevo enlace, se debe crear una entrada con un vecino que tiene un enlace asociado, en esta entrada también se debe guardar el estado de este enlace. Se debe tener en cuenta que cada vez que varía el estado del enlace se debe comprobar en la tabla que el cambio se lleva a cabo. Si no se recibe información de un enlace durante un tiempo establecido se debe borrar el enlace en cuestión y el vecino asociado.

• **Selección de MPR y señalización MPR:** La selección de los MPR sirve para seleccionar los nodos vecinos que se quiere que hagan *broadcast* de los mensajes de control. La señalización viene dada mediante mensajes “HELLO”. Cada nodo elige uno o más MPRs de manera que se asegura que a través de los MPRs seleccionados, cada nodo llega a todos los vecinos a dos saltos.

• **Difusión de mensajes de control de topología.** Estos mensajes se difunden con el objetivo de dar a cada nodo de la red la información necesaria para permitir el cálculo de rutas, son llamados mensajes TC (Topology Control). Estos mensajes que retransmite un nodo hacia sus vecinos seleccionados como MPR, tienen la información de todos sus enlaces para que los otros nodos conozcan los vecinos a los que puede llegar.

• **Cálculo de rutas:** Dada la información del estado del enlace que se adquiere mediante el intercambio de mensajes periódicos. Cada nodo mantiene una tabla de enrutamiento que permite encaminar los paquetes de datos destinados a otros nodos. Esta tabla esta basada en

la información contenida en las bases de información de enlace y de la topología. Esta tabla se actualiza cuando se detecta algún cambio en estos campos:

• El enlace

• El vecino

• El vecino de dos saltos

• La topología

Funciones auxiliares: Hay situaciones donde funcionalidades auxiliares son necesarias, como por ejemplo un nodo con múltiples interfaces, donde algunas de ellas participan en el otro dominio de enrutamiento.

Interfaces no OLSR: Hay nodos que pueden tener interfaces que no son OLSR, estas interfaces pueden ser conexiones punto a punto o conectar con otras redes. Para poder tener conectividad entre las interfaces OLSR y estas otras el router debe ser capaz de introducir información externa de encaminamiento a la red. Para esto las interfaces no OLSR crean un mensaje Host and Network Association (HNA) que contiene información suficiente para poder crear nuevas rutas con esta información.

Notificación capa enlace: OLSR no trabaja con información de capa enlace.

Sin embargo, si la información de esta capa está disponible, esta información se utiliza además de la información de los mensajes “HELLO”, para mantener información de los vecinos y los MPR. Por ejemplo: la pérdida de conectividad de la capa de enlace se puede deber a la ausencia de reconocimientos de capa de enlace.

Información redundante de topología: Para poder proveer redundancia a la información de topología, la información de anuncio que emite el nodo ha de tener información de enlaces hacia nodos vecinos que no necesariamente tengan a este nodo como MPR. El

mensaje de anuncio publica información de todos los enlaces de los nodos vecinos. Hay tres posibles niveles de redundancia:

• Sin redundancia: sólo se emite información del grupo que ha elegido a este nodo como MPR.

• Redundancia media: se emite información del grupo que ha elegido el nodo como MPR y también información de los nodos que este ha elegido como MPR.

• Redundancia alta: se emite información de todos los enlaces hacia los vecinos.

MPR redundante: Esta funcionalidad especifica la habilidad del nodo de seleccionar MPR redundantes. Aunque la redundancia crea mucho más tráfico y pierde eficiencia el mecanismo de MPR, se tiene una gran ganancia al asegurar la llegada de los paquetes a sus destinos. Esta funcionalidad es útil para situaciones en que la red tiene mucha movilidad y mantener una buena cobertura con los MPR.

Ejemplo de utilización

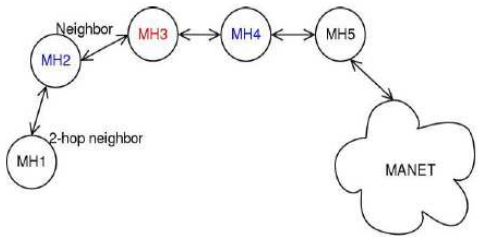

Figura II.10. Topología de red.

En este dibujo podemos ver una red con 5 nodos colocados de manera estratégica para que todos ellos tengan un vecino a cada lado. En la siguiente tabla podemos ver un ejemplo de la tabla de enrutamiento del nodo MH3

Tabla II.3. Tabla de enrutamiento del nodo MHP

		1	2	3
M	Asim.Link	MH1	MH3	
H	Sim.Link		MH1	MH1,MH3
2	2-hop neibours			MH4
M	Asim.Link		MH2,MH4	
H	Sim.Link			MH2,MH4
3	2-hop neibours			MH1,MH5
M	Asim.Link		MH3	MH3,MH5
H	Sim.Link	MH5	MH5	MH2,MH4
4	2-hop neibours			

En la tabla 3.2 podemos ver que los vecinos pueden estar en dos estados como enlace asimétrico o simétrico según la calidad de los enlaces en el momento en el que llegan los paquetes. Cada una de las columnas de la tabla indica un momento del proceso de recepción de paquetes de señalización. En la tercera columna se puede observar que ya ha llegado a converger la red. En cambio en las dos primeras columnas había nodos que no se habían detectado o incluso algunos que se habían detectado pero no se había comprobado la comunicación en ambos sentidos. También se puede ver en esta tabla como los vecinos a dos saltos son aquellos que son vecinos de algún nodo que tenemos en el estado de enlace simétrico.

2.2.2 Protocolos de ruteo basados en position-based

Esta clase de algoritmos de ruteo son paquetes enviados basados en la posición geográfica del nodo a llegar, sus nodos vecinos, y el destino. Estos protocolos requieren que cada nodo conozca su posición geográfica. La posición del destino ha ser dada por un *location service*.

Es un algoritmo simple de búsqueda, tal como el greedy forwarding puede ser usado con esta información de la posición. El paquete se envía al vecino mas cercano del nodo destino. Sin embargo el algoritmo simple de búsqueda puede acercarse pero no alcanzar el nodo destino aunque exista un enlace con el destino según lo ilustrado en la figura II.11

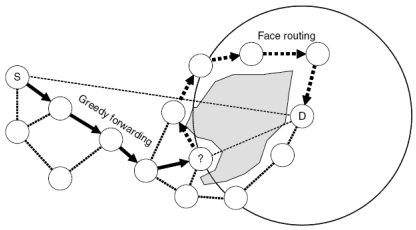

Figura II.11.Expedición basada en posición

FACE ROUTING

Se utiliza generalmente como estrategia del retraso del grafico de la red es lógicamente segmentado en donde los enlaces considerados no se cruzan con otros. Esta plantación de la red de tráfico se puede hacer localmente con algoritmos distribuidos.

Como hemos visto hasta ahora, los algoritmos basados en distancia se comportan cada vez mejor conforme aumenta la densidad, tendiendo al camino mas corto; no requieren memoria en los nodos ni en el mensaje, están libres de bucles, son de camino simple y trivialmente robustos a nodos que desaparecen o se mueven. Su gran defecto es, pues, el problema de los mínimos locales en que existe un hueco en la red que no pueden sortear. Si bien esto es solventable mediante inundaciones locales, entonces se pierde la propiedad de camino simple.

Para solventar este problema se han propuesto una serie de soluciones que se ha dado en llamar encaminamiento en facetas, teselas, perímetro, o regla de la mano derecha (face routing, perimeter routing, right-hand rule). La idea que subyace al encaminamiento en facetas es la siguiente: tómese un grafo plano (esto es, cuyas aristas no se cortan) arbitrario. Llamamos faceta o tesela a cada polígono delimitado por las aristas del grafo (Ver

Fig.II.12). Tenemos f facetas, de las cuales f − 1 son finitas y una de ellas es infinita; esta ultima es la faceta exterior que envuelve a todas las demás. Si tenemos dos nodos origen y destino y los unimos con una recta imaginaria, esta recta interfecta con un subconjunto de facetas. La regla de la mano derecha nos dice que si seguimos una figura poligonal manteniéndonos siempre en contacto con la mano derecha en la “pare”, la rodearemos en sentido horario si estamos en el exterior, o en sentido antihorario si estamos en el interior. En cualquier caso, el dato relevante es que antes o después regresaremos al punto de origen.

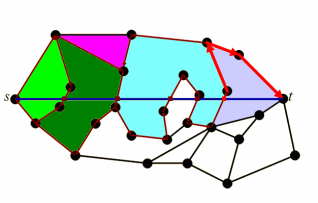

Figura II.12. Encaminamiento en grafos planos mediante facetas

Sabiendo esto, el paquete parte del nodo origen y se envía a recorrer la faceta que contiene dicho nodo y que está más próxima al destino, intersecando la recta Origen-Destino. De algún modo se determina otro nodo en esta faceta que también pertenece a la siguiente faceta más próxima al destino, y allí se efectúa un cambio de faceta hacia el destino. Si el grafo es conexo, se puede probar que se alcanzaría el destino en un número finito de pasos. No hay que olvidar que estamos considerando también la faceta infinita.

A la vista de estos primeros resultados queda claro que los algoritmos en la familia FACE son costosos en comparación con los voraces. Su ventaja radica en la garantía de entrega.

GPSR

Uno de los primeros protocolos de ruteo position-based prácticos para las redes inalámbricas es el Greedy Perimeter Stateless Routing mas conocido por sus siglas como (GPSR). El GPRS combina el greedy forwarding con el fase routing fallback. GPSR, es un protocolo que reacciona rápidamente, además de un eficiente protocolo de ruteo para redes móviles inalámbricas. Este algoritmo es distinto a los algoritmos de ruteo antes mencionados , que utilizan nociones gráficoteóricas 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 a el forwarding de los paquete. GPSR utiliza *greedy forwarding* para remitir los paquetes a los nodos que están siempre progresivamente más cercano a el destino. En las regiones de la red donde no existe una camino greedy (es decir, la única trayectoria requiere que un movimiento temporalmente se encuentre mas lejos del destino), GPSR se recupera por la busqueda en perimeter mode, en el cual un paquete atraviesa caras sucesivas más cercanas de un subgraph planar del gráfico de radio completo en la conectividad de la red, hasta alcanzar un nodo más cercano a necesitada (nodo destino), donde el greedy forwarding termina.

GPSR permitirá la construcción de las redes que no pueden escalar con los algoritmos anteriores del encaminamiento para las wire networks y wireless network. Tales clases de redes incluyen:

Rooftop networks:(Redes del tejado) despliegue fijo, denso de números extensos de nodos.

Redes ad hoc: densidad móvil, que varía, ninguna infraestructura fija

Redes del sensor: densidad móvil, potencialmente grande, números extensos de los nodos, recursos empobrecidos del por-nodo

Redes de vehículos: densidad móvil, no-energía-obligada, movilidad.

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

La mayor ventaja de GPRS no es la tecnología en si misma sino los servicios que facilita. Los terminales de este nuevo sistema permiten personalizar funciones, desarrollar juegos interactivos, e incorporan aplicaciones para el intercambio de mensajes y correos electrónicos, a los cuales se podrá acceder directamente sin la necesidad de conectarse a Internet. Incorporan además una ranura para introducir la tarjeta de crédito con chip que facilitará las transacciones electrónicas más seguras. Con la tecnología GPRS se da un paso hacia la localización geográfica, en función de donde se encuentre el usuario, la operadora le puede ofrecer mayor información de la zona.

2.2.3.- Hybrid wireless mesh protocol (HWMP)

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

La realización de HWMP es una adaptación de ruteo reactivo al protocolo AODV, a la capa 2 y a la métrica radio-aware llamada la radio métrica AODV (RM-AODV). Un nodo mesh, generalmente un portal mesh, puede ser configurado periódicamente anunciando una difusión, que es fijado en la cima que la cual permite el ruteo proactive hacia este portal en mallado.

La parte reactiva de HWMP sigue los conceptos generales de AODV según lo descrito antes. El protocolo HWMP Utiliza el método de vector distancia y el proceso de descubrimiento de la ruta con la petición de la ruta y su respuesta respectiva. Los números de serie de la destinación se utilizan a reconocer la vieja información de ruteo. Sin embargo, hay significativas diferencias en los detalles. La Figura II.13. muestra la estructura de la Petición de la ruta de HWMP para ilustrar las nuevas características.

HWMP utiliza direcciones MAC como protocolo de ruteo para la capa 2 en vez de direcciones IP. Además, HWMP puede hacer uso de una métrica de ruteo más sofisticada que el hopcount tal como métricas radio-aware. Un campo métrico de la nueva trayectoria es incluida en los mensajes de RREQ/RREP que contiene el valor acumulativo de los enlaces métricos de la trayectoria hasta ahora. El ruteo por default métrico de HWMP es el

airtime métrico donde las métricas separadas del enlace se agregan hasta conseguir la trayectoria métrica.

Puesto que los cambios métricos radio-aware son utilizados mas a menudo que el hopcount métrico, es preferible tener solamente el destino a contestar a RREQ de modo que la trayectoria métrica sea actualizada. Por esta razón, la flag de la destinación solamente es fijada (DO=1) por default en HWMP.

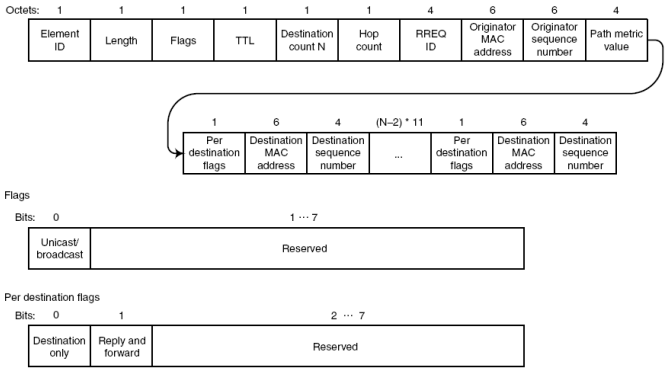

Figura II.13. Ruta de petición HWMP

Explícitamente fijando la bandera de el destino solamente DO=0, es posible dejar nodos intermediarios para la respuesta. Esto da un estado latente más corto para descubrimiento de la ruta. Pero el camino métrico no está actualizado. Por lo tanto, el nodo intermedio que contestó con un RREP remitirá el RREQ a el destino. Esto es controlado por una respuesta y una forward flags. También es fijada por el defecto (RF=1), pero puede ser un set (variable) para conseguir el comportamiento tradicional de AODV. La bandera de el destino serà fijada en el RREQ remitido.(DO=1). Esto evita que otros nodos intermedios generen las contestaciones de la ruta y que pudieran ser muchas.

Cualquier información de encaminamiento recibida (RREQ/RREP) se comprueba para saber si hay validez con una comparación número de serie (sequence number). La información de encaminamiento es válida si el número de serie no es más pequeño que el número de serie en la información anterior. Si los números de serie son iguales y la información de ruteo, que es la trayectoria métrica, es mejor, entonces la nueva información será utilizada y el nuevo mensaje será procesado

.HWMP puede utilizar el mantenimiento RREQs periódico para mantener una mejor trayectoria métrica entre la fuente y el destino de trayectorias activas. Esto es una característica opcional. HWMP permite destinos múltiples en los mensajes de RREQ, que reduce los gastos indirectos del ruteo cuando un nodo mesh tiene que encontrar las rutas a varios nodos simultáneamente. Éste es el caso para reparar enlaces rotos y para el mantenimiento RREQs.

Algunas flags pueden tener valores diferentes para cada destino. Por esta razón, flags destinadas son asociadas con cada destino y secuencia numérica. Esas son las flags específicamente relacionadas a la generación de los mensajes RREP. Un campo explícito del Time to Live (TTL) es necesario, puesto que no hay nada en la cabecera como en AODV tradicional. El uso de la extensión preactiva a RM-AODV es configurable. La extensión proactive utiliza la misma metodología vector distancia como RM-AODV y hace uso mensajes de ruteo de RM-AODV.

Utilizar la extensión proactive, por lo menos un portal mesh tiene que estar configurado para difundir periódicamente broadcast del portal mesh. Esto acciona una selección de la

raíz y un proceso del mediador, fuera de los cuales un solo portal de la raíz se desarrolla. El portal fija el tipo de aviso de la bandera a 1 (raíz) en sus avisos periódicos del portal del acoplamiento. En recibo de el aviso del porta de la raíz, un nodo mesh instalará una camino al portal de la raíz, un nodo mesh que recibió el aviso portal de la raíz con la mejor trayectoria métrica. Una camino al portal mesh es anunciado, se puede también instalar en el recibo de avisos portal con el tipo flag del aviso fijada a 0 (portal). La disposición de la trayectoria conducirá a un árbol fundamentado en el portal de la raíz (acoplamiento).

Si la bandera de registro no se fija en el mensaje del aviso (non-register mode), el proceso de los avisos de raíz son paradas aquí. Cuando un nodo mesh desea enviar tramas de los datos portadle la raiz, puede enviar un RREP gratuito al portal de la raíz inmediatamente antes del primer paquete de datos. Esto instalará el camino el portal de la raíz al nodo de la fuente.

Si la bandera del registro se fija en el mensaje del aviso (registration mode), el nodo mesh espera cierto rato para la raíz adicional los mensajes llegados pudieron también publicar un RREQ18 con TTL=1 explícitamente para pedir a sus nodos vecinos rutas a la raíz portal. El nodo mesh elige la trayectoria con la mejor trayectoria métrica a el portal de la raíz. Se coloca con el portal de la raíz enviando un gratuito RREP al portal de la raíz. El registro tiene que ser cada vez que el nodo cambia su nodo original. Una descripción de las diversas opciones de la configuración de HWMP es demostrado en la Fig.II.14.

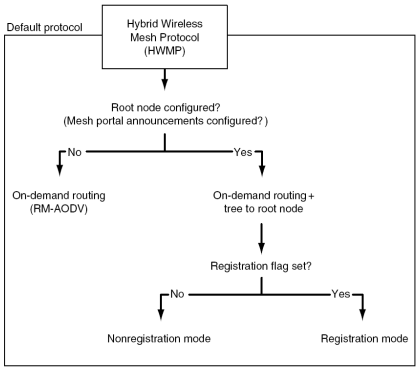

Fig II.14 Configurabilidad de HWMP

2.3.- SEGURIDAD EN WMN

2.3.1.- USO DE LAS CAPAS DEL MODELO OSI EN REDES MESH

2.3.1.1.- Capa física

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

Estos mecanismos son la selección dinámica de frecuencia (DFS) y el control de potencia (TPC). Con el fin de aumentar la capacidad, mitigar la atenuación, delay e interferencia entre canales, se han creado sistemas multi-antenas como es el caso de las antenas pequeñas y los sistemas MIMO que hace uso de esta tecnología con fin de conseguir capacidades superiores a los 108 Mbps en el enlace inalámbrico. Por otro lado existen otras tecnologías

de radio que usan las técnicas como son el acceso múltiple de la frecuencia ortogonal (OFDM) y Banda ultra-ancha (UWB).

2.3.1.2.- Capa Mac

Existen grandes diferencias entre la capa de acceso al medio en una WMNs y las contrapartes clásicas de las redes inalámbricas. Las redes clásicas poseen serias limitaciones en los multisaltos debido a los problemas del nodo oculto y el nodo expuesto.

Existen mecanismos de acceso al medio que son muy útiles para las redes Mesh como es el caso de TDMA (Time Division Multiple Access) y CDMA (Code Division Multiple Access) los cuales pueden disminuir los efectos de las interferencias, ya que dos nodos pueden ocupar simultáneamente el mismo empleando códigos diferentes.

Protocolos convencionales

La principal responsabilidad de los protocolos de la capa MAC es asegurar el compartimiento de recursos. Hay dos grandes categorías de los esquemas MAC como son los protocolos basados en contención y los protocolos basados en libres colisiones de los canales.

Los protocolos basados en contención asumen que no hay entidad central que asigne los canales en la red. Para transmitir cada nodo debe contener su propio medio. Las colisiones resultan cuando más de un nodo trata de transmitir al mismo tiempo. Como es bien sabido los protocolos basados en contención incluyen Aloha, CSMA y CSMA/CA. En contraste, los protocolos de libre colisión asigna canales dedicados a cada nodo que desea

comunicarse. Los protocolos de libre colisión pueden eliminar colisiones con eficacia, liberando asi los canales de alto trafico. Ejemplos de estos protocolos son el TDMA, CDMA y FDMA.

ALOHA y SLOTTED ALOHA

La importancia de ALOHA se basa en que usaba un medio compartido para la transmisión. Esto reveló la necesidad de sistemas de gestión de acceso como CSMA/CD, usado por Ethernet. A diferencia de ARPANET donde cada nodo sólo podía comunicarse con otro nodo, en ALOHA todos usaban la misma frecuencia. Esto implicaba la necesidad de algún tipo de sistema para controlar quién podían emitir y en qué momento. La situación de ALOHA era similar a las emisiones orientadas de la moderna Ethernet y las redes Wi-Fi.

En Aloha, cada estación transmite los mensajes conforme le van llegando, de modo que si más de una estación tiene mensajes para transmitir, los paquetes colisionan en el canal destruyéndose. Cada estación interpreta que se ha producido colisión si al vencer un determinado temporizador de time out, no se ha recibido reconocimiento del mensaje enviado. De este modo, tras la colisión, cada estación retransmitirá el mensaje transcurrida una cantidad de tiempo aleatoria. Hay que señalar que aunque solamente una parte del paquete transmitido haya sido destruido (colisión parcial), la estación retransmitirá el paquete completo. El inconveniente es que, si la red está saturada, el número de colisiones puede crecer drásticamente hasta el punto de que todos los paquetes colisionen. Para ALOHAnet el uso máximo del canal estaba en torno al 18%, y cualquier intento de aumentar la capacidad de la red simplemente incrementaría el número de colisiones, y el

rendimiento total de envío de datos se reduciría, fenómeno conocido como colapso por congestión.

En aloha ranurado los mensajes se transmiten sólo en determinados intervalos de tiempo llamados slots, lo cual tiene el efecto de doblar el rendimiento efectivo del sistema puesto que en este caso los paquetes, ó no sufrirán colisión, ó la colisión afectara al paquete completo (dos o más estaciones transmitiendo sobre el mismo slot). Los mecanismos de detección de colisiones son mucho más difíciles de implementar en sistemas inalámbricos en comparación con los sistemas cableados, y ALOHA no intentó siquiera comprobar las colisiones. En un sistema cableado, es posible detener la transmisión de paquetes que colisionen, detectando primero la colisión y notificándolo a continuación al remitente. En general, esta no es una opción viable en sistemas inalámbricos, por lo que ni siquiera se intentó en el protocolo ALOHA.

VENTAJAS DE ALOHA RANURADO SOBRE ALOHA PURO

• La eficiencia de este protocolo es el doble que la del protocolo aloha puro

• Se adapta a un número variable de estaciones

DESVENTAJAS DE ALOHA RANURADO

• Se requiere de sincronización entre estaciones para determinar

• Requiere almacenar la trama transmitida debido a posibles retransmisiones

CSMA/CD

El protocolo CSMA/CD (Acceso Múltiple con Escucha de Portadora y Detección de Colisiones) es una técnica usada en redes Ethernet para mejorar sus prestaciones. Anteriormente a esta técnica se usaron las de Aloha puro y Aloha ranurado, pero ambas presentaban muy bajas prestaciones. Por eso apareció primeramente la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD. Significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha el canal antes de emitir. CSMA/CD supone una mejora sobre CSMA, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión, para inmediatamente la transmisión. La ganancia producida es el tiempo que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

Protocolos IEEE 802.11 CDF

DCF esta basado en CSMA/CA y opera de manera similar. Un nodo que desea trasmitir primero sensa el canal. Si se encuentra el medio ocupado, se sensa hasta encontrarlo libre.

Figura II.15. Censado del canal de CFS

Si el medio esta libre para un determinado periodo de tiempo llamado DIFS (distributed inter frame space) el nodo puede transmitir.

SI el receptor recibió correctamente el paquete este envía un mensaje ACK

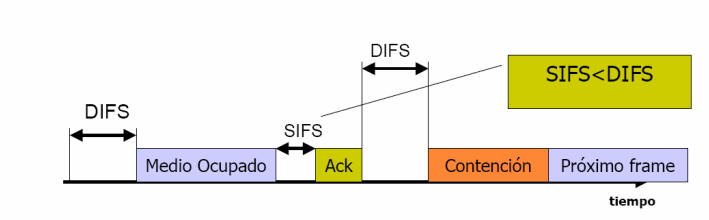

Figura II.16. Mecanismo de transferencia Datos y ACK

Si el ACK no es recibido el transmisor asume que ha ocurrido una colisión y doblega el tamaño del paquete de su ventana de contención. Luego el transmisor escoge un número de random Back-off entre cero y su ventana de contención.

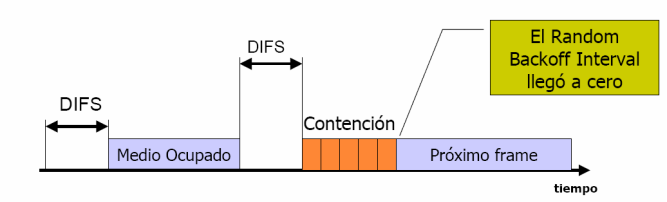

Figura II.17. Ventana de contención en CFS

El transmisor permitirá la transmisión del paquete cuando el canal es libre para un DIFS aumentado por el tiempo random back-off. El paquete se cae después de un número dado de retransmisiones fallidas. Para reducir las coliciones, el estándar define un mecanismo de sensado de portadora. Un nodo que desea transmitir, primero transmite un paquete pequeño de control llamado RTS, el cual incluye fuente, destino y duración de transmisión del

paquete. Si el medio esta libre el receptor responde con un mensaje CTS que incluye la duración del paquete de datos y su ACK.

Cualquier nodo esta recibiendo el RTS y/o CTS se asigna un vector (NAV) el da la duración. Una vez pasa esto el NAV cuenta en forma decreciente hasta llegar a cero. Un nodo no puede transmitir hasta que el NAV no llegue a cero. La información de la duración llevada por el RTS protege el transmisor de colisiones cuando recibe el ACK.

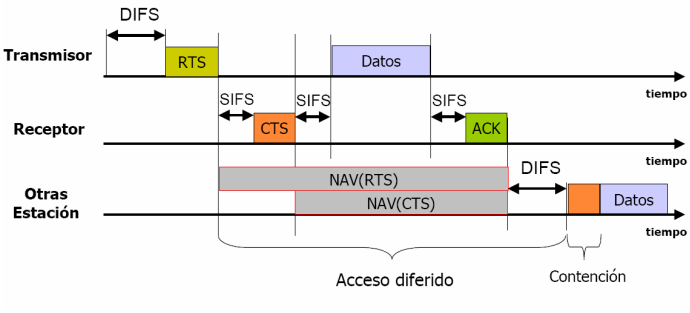

Figura II.17. Network Allocation Vector (NAV)

Protocolos IEEE 802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

(EDCA) Enhanced Distributed Channel Access y (HCCA) Controlled

Access.

El denominado EDCA es el acceso con contención que representa una evolución del acceso DCF del estándar IEEE 802.11. Por el otro lado el HCCA corresponde al acceso sin contención basado en polling. Obviamente, el nuevo modo de operación HCCA, en tanto que considera un control acceso centralizado, supone la mejor alternativa para soportar la QoS. Sin embargo los sistemas centralizados suponen más complejidad, no son eficientes para transmisiones de datos y necesitan sincronización. Es por ello que el modo centralizado PCF del IEEE 802.11, predecesor del HCCA, apenas ha sido implementado, lo que sin duda cuestiona la futura implementación del modo HCCA. A pesar de los posibles inconvenientes en términos de QoS, el acceso con contención es más sencillo, fácil de instalar y no supone gran coste en cuanto a mantenimiento y gestión. Además su uso, tipo "plug and play" es más cómodo para el usuario, por lo que es previsible que, al menos inicialmente, el estándar IEEE802.11e centre su desarrollo en el modo EDCA. Por consiguiente el desarrollo de técnicas de gestión de recursos que garanticen la QoS cuando se opera en contención con el mecanismo EDCA resulta imprescindible. Al mismo tiempo, y debido a su naturaleza, la gestión de recursos radio en EDCA supone también un desafió relevante. Como la operación de HCCA y PCF requieren una central de control y sincronización entre nodos y esto es complicado para las redes Mesh, por este motivo hay que fijar la atención en EDCA.

Protocolos Mac avanzados para WMNs

Los protocolos diseñados para WMNs asumen antenas omnidirecionales que transmiten señales de radio y reciben señales de todas las direcciones. Cuando dos nodos se están comunicando, todos los otros nodos de entre los vecinos tienen que seguir siendo silenciosos, mientras tenga un impacto negativo en la capacidad21. De otro modo la capacidad disminuye con el aumento del número de nodos. Con las antenas direccionales (antenas elegantes incluyendo), dos pares de nodos situados en de cada uno de los radios vecinos puede comunicarse potencialmente y simultáneamente, dependiendo en las direcciones de la transmisión. Para nodos equipados con antenas direccionales, ocurre el problema del nodo oculto que ocurre cuando dos transmisores están cerca y sus antenas apuntan en diferentes direcciones, entonces estos son invisibles entre ellos mientras se causan colisiones en el receptor. Existen cinco problemas que se plantean al usar antenas direccionales como son el Nodo expuesto direccional, Desconocimiento del estado del canal, Nodos ocultos debido a asimetría en ganancia, Formas de las regiones “silenciosas” y “Deafness”.

Nodo expuesto direccional

A quiere enviar un paquete a B, y E quiere enviar un paquete a C. El nodo A envía el RTS direccionalmente al nodo B, pero esta transmisión la oye el nodo de manera que no puede enviar el paquete aun no interfiriendo en la comunicación A-B. El nodo E está direccionalmente expuesto.

Desconocimiento del estado del canal

A está transmitiendo un paquete a D después del envío RTS-CTS. El nodo E que no escucha esta transmisión decide enviar un RTS al nodo B. Cuando A acaba de transmitir, decide enviar al nodo F ya que no sabe que hay una Comunicación entre E y B. A interfiere en esta comunicación. Éste sería un caso de desconocimiento del estado del canal del nodo A.

Nodos ocultos debido a asimetría en ganancia

El nodo B envía un RTS direccional (DRTS) al nodo F. El nodo F responde con un CTS direccional (DCTS) de ganancia Go. El nodo A tiene un paquete a Transmitir al nodo E. Y determina el canal libre ya que no le llega la potencia de la antena F. El nodo A por lo tanto envía un DRTS con ganancia Gd al nodo E que sí oye la transmisión del nodo F. De esta manera hay interferencia y por lo tanto colisión de paquetes y los datos no llegan correctamente al receptor.

Formas de las regiones "silenciosas"

Debido al aumento de la ganancia en antenas direccionales las formas de las zonas "silenciosas" o sin cobertura son diferentes en antenas omnidireccionales y antenas direccionales. Esto afecta indirectamente en características topológicas como patrones de tráfico y ancho del lóbulo de la transmisión direccional.

“Deafness”

Para explicar este problema debido al uso de antenas direccionales, utilizaremos el escenario de la Fig. 4.5. Los nodos C y D quieren transmitir al nodo B a través del nodo E. Si E responde el paquete de D, C no lo sabría con DMAC y transmitiría un RTS a E. E al tener el lóbulo dirigido a D no recibe el RTS de C. De manera que E vuelve a retransmitir. E está “sordo” ya que no

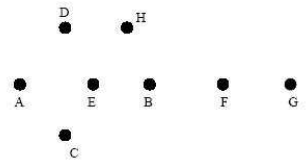

Figura II.18. Escenario ejemplo de nodos ocultos debidos a asimetría en Ganancia.

Oye las transmisiones del nodo C en otra dirección. Esto provoca un desperdicio de la capacidad de la red en envíos de paquetes de control innecesarios. A diferencia de estos nodos están los que están equipados con antenas omnidireccionales, en los cuales el problema del nodo oculto no ocurre. El problema deafness ocurre cuando falla la comunicación entre el transmisor y el receptor porque el receptor esta escuchando en otra dirección.

La interferencia direccional22 alta es causada por la alta ganancia en las antenas. Para estos problemas están algunos protocolos MACs basados en la 802.11 DCF el cual comprende RTS, CTS, DATA y ACK. El DCF transmite los mensajes de control y datos omnidireccionalmente con antenas direccionales. Se pueden manejar antenas direccionales usando diferentes combinaciones de mensajes direccionales y omnidireccionales. Los

protocolos MAC donde se utilizan las antenas direccionales se denominan Direccional-MAC (DMAC).

Antenas usadas en la capa Mac

Existen dos esquemas importantes que son utilizados en esta capa como son: las antenas MACs direccionales y las antenas MACs con energía controlada. Por otro lado el IEEE esta trabajando en el estándar 802.11s y propone el MMAC (Multichannel MAC) y HMCP (Hybrid Multichannel Protocol). En MMAC se emplean varios canales con una sola interfaz de radio, por lo que se requiere señalización y coordinación con el fin de que todos los nodos escuchen el cana adecuado en cada momento. Por otra parte en HMCP los nodos tienen varias interfaces, unas trabajan en canales fijos y otros variables, empleando los canales fijos para control y señalización.

Antenas MACs direccionales: El primer sistema elimina todos los nodos expuestos si la viga de la antena se asume como perfecta. Sin embargo, debido a la transmisión direccional, se producen nodos ocultos. Estos esquemas también hacen frente a otras dificultades tales como costo, complejidad del sistema, y sentido práctico de antenas direccionales orientables rápidas.

Antenas MACs con energía controlada: Este sistema reduce nodos expuestos, usando energía baja de la transmisión, y mejora así el factor espacial de la reutilización del espectro en WMNs. Sin embargo, la aplicación de los nodos ocultos puede llegar a ser peor porque una transmisión baja más el nivel de la energía y reduce la posibilidad de detectar un nodo potencial que interfiere. Proponer protocolos innovadores en la capa MAC, no es una buena

solución sabiendo que se tiene una pobre escalabilidad en una red multi-hop, en este caso es imprescindible el uso de los protocolos TDMA y CDMA.

Diseño de un protocolo MAC 802.11 con antenas Direccionales Rehúso espacial: En anteriores estudios se confirma que el uso de antenas direccionales aumenta el rehúso espacial con el uso de un protocolo MAC Específico para antenas direccionales.

Mayor alcance: Además, el uso de antenas direccionales permite tener un mayor alcance a los nodos de la red. Todas las transmisiones son direccionales ya que de esta manera se utiliza todo el rango de cobertura posible con antenas direccionales y no se ocupa el canal innecesariamente con Transmisiones omnidireccionales.

NAV direccional: Adaptando el mecanismo de NAV a antenas direccionales se diseña un mecanismo para que los nodos vecinos puedan conocer si hay una transmisión que puedan dañar y así retrasar su intento de transmisión.

Tabla de localización: La localización de los nodos no se asume a priori a diferencia de los antiguos protocolos ya que existe un mecanismo que informa a los nodos de la localización de los nodos vecinos.

Solución a los nodos ocultos: Este protocolo aporta una solución para reducir el problema de nodos ocultos que aparece al utilizar antenas direccionales. De esta manera, el número de colisiones será menor y aumentará el *throughput*.

RTS circular

Este protocolo está basado en el envío de RTS circular. La transmisión del RTS es direccional y se envía consecutivamente y circularmente a todos los nodos vecinos. Se asume que todos los nodos tienen un máximo de antenas que cubre el área del transmisor. Primero se envía un RTS en una dirección predefinida como es la primera antena direccional, la antena 0. Seguidamente se envía un RTS en la dirección de la segunda antena, 1. Se envía un RTS en las direcciones de las antenas hasta llegar al máximo de antenas. Cuando el nodo transmisor acaba de enviar todos los RTS por todas las antenas del nodo y, por lo tanto el nodo receptor habrá recibido el RTS, se envía el CTS direccional. En este protocolo el envío del CTS también es circular a diferencia de [6] que explicamos en la siguiente sección.

El uso de RTS y CTS circular va a resolver el problema de nodos ocultos. Además permite mantener actualizada una tabla de localización con lo que no es necesario un sistema extra de localización, como podría ser Global Positioning System (GPS). En contrapartida, el uso del RTS y el CTS circular va a alargar el tiempo de una transmisión ya que se necesitan más slots times para hacer el recorrido circular.

Si al añadir los mecanismos de RTS y CTS circular el tiempo necesario para efectuar una transmisión se alarga, significa que el *throughput* va a ser menor. Sin embargo, la principal ventaja del uso de antenas direccionales, como se ha comentado anteriormente, es que permiten que más de dos parejas de nodos se comuniquen al mismo tiempo aún así estando próximos. Este efecto se ha denominado “rehúso espacial”. Esta ventaja va a significar un

aumento del *throughput* total del sistema y aunque ahora con este nuevo esquema el tiempo para realizar una transmisión sea mayor, el *throughput* que se consigue gracias Al rehúso espacial va a ser mayor. Ante este nuevo esquema se espera que cuantos más nodos y cuanto mayor sea el número de antenas direccionales, el Rehúso espacial hará que el *throughput*23 aumente cada vez más exponencialmente. En definitiva, cuanto mayor es el número de nodos y cuanto Mayor es el número de antenas direccionales en cada nodo, mayor es el número de posibles combinaciones de parejas de nodos que pueden comunicarse a la vez. Continuando con la explicación del RTS circular, cuando los nodos vecinos reciben el RTS sabrán si deben retrasar su intento de transmisión con un mecanismo que se detalla más adelante.

Una vez se envía el último RTS el transmisor escucha el medio omnidireccionalmente a la espera de la recepción del CTS del nodo receptor. Si éste llega antes de un tiempo predefinido (CTS timeout), el receptor envía los datos y el receptor envía el ACK. El paquete de datos y el de ACK son enviados de la misma manera que en el tradicional protocolo MAC 802.11, pero con la diferencia que todas estas transmisiones se realizan con antenas direccionales. Es decir, la segunda gran ventaja del uso de antenas direccionales es que su alcance es mayor. Las antenas direccionales concentran toda la energía en una sola dirección, obteniendo un diagrama de radiación en el que el lóbulo principal está enfocado en la dirección de interés y el resto de los lóbulos quedan minimizados. Como conclusión, una antena direccional puede llegar a transmitir a nodos más lejanos que una antena omnidireccional con la misma Cantidad de energía disponible para la transmisión. Y, por lo tanto, también una antena direccional necesita menos energía para transmitir a un nodo que

esté a una distancia alcanzable por una antena omnidireccional. Para conseguir esto último sería necesario un esquema de control de la potencia de transmisión de la antena. La Fig.II.19 muestra el mecanismo del RTS circular. Este mecanismo se describe en la siguiente sección, junto al mecanismo del CTS circular.

CTS circular

El esquema del CTS circular es el mismo que el del RTS circular. Cuando el nodo receptor recibe el RTS, y después del envío del RTS por la última antena del nodo transmisor, el nodo receptor envía el CTS en la dirección del nodo transmisor. Seguidamente se envía un CTS por todas las antenas e informa de esta manera a los nodos vecinos que hay una transmisión. En la Fig.II.19 el nodo 2 tiene un paquete para el nodo 4. De manera que envía un RTS al nodo 4 por la antena 0 y posteriormente envía un RTS por la antena 1 a los nodos vecinos para informar de la transmisión. De manera que los nodos 0, 1 y 3 serán informados de dicha transmisión, Cuando se envía el RTS por la última antena, si el nodo receptor, 4, lo recibe correctamente, se envía un CTS en la dirección del nodo transmisor con la antena 1. Seguidamente el nodo receptor envía el CTS por la antena 0 y los nodos 5 y 6 serán informados de la transmisión. Si el envío del CTS no fuera circular los nodos 5 y 6 no estarían informados de la transmisión y podrían intentar enviar un paquete por la antena 1 y destruir la comunicación. Con el envío del CTS circular hay más nodos informados de la comunicación de manera que se reducen los nodos ocultos y de esta manera las colisiones.

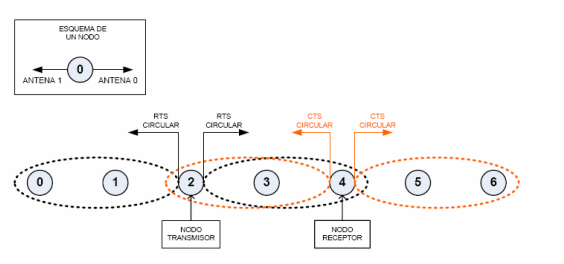

Figura II.19. Mecanismos de RTS Circular y CTS Circular

Tabla de localización

Al utilizar RTS circular, este protocolo asegura que el RTS llega al nodo receptor. El RTS al llegar al nodo receptor podrá saber por diversidad selectiva la dirección por la cual ha recibido el RTS y así poder localizar dónde está el nodo transmisor. De la misma manera el nodo transmisor con la recepción del CTS puede saber la localización del nodo receptor.

Cada nodo tiene una tabla de localización como es explicada anteriormente. La tabla informa de qué nodo se trata, el nodo por el que se ha escuchado el paquete, la antena por el cual el transmisor escuchó el paquete y la antena por el cual el receptor escuchó el paquete. En la Tabla II.4 podemos ver la tabla de localización del nodo 0 correspondiente a la Fig. II.20. El nodo 0 puede ver al nodo 1 por la antena 0 y el nodo 1 con la antena 4. El nodo 0 puede ver al nodo 2 por la antena 5 y el nodo 2 con la antena 1. Y finalmente, puede ver al nodo 3 por la antena 6 y el nodo 3 con la antena 2.

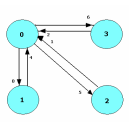

Figura II.20. Envío de RTS y CTS

Tabla II.4. Tabla localización Nodo 0 de la Fig II.20

Nodo	Vecino	Antena	Antena del vecino
0	1	0	4
0	2	5	1
0	3	6	2

Al principio esta tabla está vacía. La tabla de localización se actualiza en cada recepción por la movilidad de los nodos. Esta información es importante para la Decisión de los nodos vecinos en enviar un paquete o atrasar esta transmisión.

2.3.1.3.- Capa de red

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

• Métrica de funcionamiento múltiple: Consiste en escoger la trayectoria adecuada para el envío de paquetes.

• Escalabilidad: Se requiere el uso de un protocolo que perdure mucho tiempo en funcionamiento y que sea útil para las nuevas tecnologías, puesto que las WMNs aun no se han explorado por completo.

• Robustez: Consiste en Evitar la interrupción del servicio, WMNs debe ser robusto para ligar faltas o la congestión. Los protocolos del encaminamiento también necesitan hacer balanceo de la carga.

• Infraestructura Mesh con ruteo eficiente: Los protocolos de encaminamiento se espera que sean más simples que los protocolos de una red Ad Hoc. Con la infraestructura Mesh proporcionada por los routers, el protocolo de ruteo para clientes Mesh pueden ser más simple.

De acuerdo a estas características se recomienda el uso de MANET (Mobile Ad-Hoc Networks) del IETF, que tiene dos tipos de protocolos: activos como es el caso de AODV (Ad-Hoc ondemand Distance Vector) y preactivos como es el OLSR (Optimizad Link State Routing).

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

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

• **Encaminamiento de Multi-Radio:** un multi-radio LQSR es una nueva métrica que asume que todas las radios en cada nodo están templadas a los canales que no interfieren con la asignación que cambia infrecuentemente.

• **Encaminamiento multidireccional:** Los objetivos principales con este tipo de encaminamiento es hacer una carga se balancee mejor y proporcionar alta tolerancia de avería. Las trayectorias múltiples se seleccionan entre la fuente y el destino. Cuando un

acoplamiento está quebrado en una trayectoria debido a una mala calidad o movilidad del canal, otra trayectoria en el sistema de trayectorias existentes puede ser elegida. Así, sin esperar al sistema para arriba una trayectoria nueva del encaminamiento. Sin embargo, dado un funcionamiento métrico, la mejora depende de la disponibilidad de las rutas entre la fuente y la destinación. Otra desventaja del encaminamiento multidireccional está su complejidad.

• **Encaminamiento Jerárquico:** Este tipo de encaminamiento se emplea para agrupar nodos de red en racimos. Cada racimo tiene una o más cabezas del racimo. Los nodos en un racimo pueden tener uno o más saltos a una distancia lejana de la cabeza del racimo. Puesto que la conectividad entre los racimos es necesaria, algunos nodos pueden comunicarse con más de un racimo y trabajar como entrada. Cuando la densidad del nodo es alta, los protocolos del encaminamiento hierarchical tienden para alcanzar un funcionamiento mucho mejor debido hay menos trayectoria y procedimiento es más rápido debido la disposición de encaminar la trayectoria. Sin embargo, la complejidad de mantener la jerarquía puede comprometer el funcionamiento del protocolo del encaminamiento. Por otra parte, en WMNs, un cliente de acoplamiento debe evitar de ser una cabeza del racimo porque puede convertirse en un embotellamiento debido a su capacidad limitada.

• **Encaminamiento Geográfico:** consiste en proyectar los paquetes delanteros solamente usando la información de la posición de nodos en la vecindad y el nodo de destino25. Así, el cambio de la topología tiene menos impacto en el encaminamiento geográfico que los otros protocolos del encaminamiento. Los algoritmos geográficos son un tipo de esquemas codiciosos del encaminamiento de una sola trayectoria en los cuales la decisión de la

expedición de paquete se hace basándose en la información de la localización del nodo de la expedición, sus vecinos, y el nodo de destino. Sin embargo, todos los algoritmos codiciosos del encaminamiento tienen un problema común, es decir, la entrega no está garantizada aunque exista una trayectoria entre la fuente y el destino.

2.3.1.4.- Capa de transporte

Hasta el momento, no se ha propuesto ningún protocolo del transporte específicamente para WMNs. Sin embargo, una gran cantidad de protocolos del transporte están disponibles para las redes ad hoc. Estudiar estos protocolos ayuda en el diseño de los protocolos del transporte para WMNs. Diversos protocolos del transporte son necesarios para ser usados en tiempo real como es el caso del tráfico tráfico. Transporte confiable de los datos: Los protocolos confiables del transporte se pueden clasificar más a fondo en dos tipos: Variantes del TCP y nuevos protocolos del transporte. Las variantes del TCP mejoran el funcionamiento del clásico TCPs abordando los problemas siguientes:

• **Pérdidas del paquete de la No-Congestión:** El TCPs clásico no puede distinguir las pérdidas de la congestión y la no congestión. Como resultado, cuando ocurren las pérdidas de la no-congestión, el rendimiento de la red cae rápidamente debido a la evitación innecesaria de la congestión. Además, cuando los canales inalámbricos vuelven a la operación normal, el TCP clásico no se puede recuperar rápidamente. Se puede utilizar un mecanismo de la regeneración para distinguir diversas pérdidas del paquete.

• **Falta desconocida del acoplamiento:** La falta del acoplamiento ocurre con frecuencia en las redes ad hoc móviles, puesto que todos los nodos son móviles. Por lo que en las WMNs,

la falta del acoplamiento no es tan crítica como en redes ad hoc móviles. Debido a los canales y a la movilidad Inalámbrica en clientes de acoplamiento, la falta de acoplamiento inmóvil puede suceder.

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

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

2.3.1.5.- Capa de aplicación

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

Acceso a Internet: Los usos variados del Internet proporcionan información oportuna, para hacer la vida más confortable, y para aumentar eficacia y productividad del trabajo. En un hogar o un ambiente de negocio pequeño o mediano, la solución del acceso de la red más popular es un módem inmóvil de DSL o de cable junto con IEEE 802.11 puntos de acceso. Sin embargo, comparado con este acercamiento, WMNs tiene muchas ventajas potenciales: un costo más bajo, una velocidad más alta, y una instalación más fácil. Almacenaje y compartimiento de información distribuida: tener acceso a Backhaul en Internet no es necesario en este tipo de uso, y los usuarios se comunican solamente dentro de WMNs. Un

usuario puede desear almacenar datos en grandes cantidades en los discos poseídos por otros usuarios, archivos de la transferencia directa discos de otros usuarios los cuales están basados en mecanismos del establecimiento de una red del par-a-par. Los usuarios dentro de WMNs pueden también desear charlar, hablar en los teléfonos de video, y los jugar en línea con varias personas.

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

Mejorar los protocolos de cada capa existentes que están en uso: En una red inalámbrica, los protocolos en las capas más bajas no pueden proporcionar la ayuda perfecta para la capa que este en uso. Por ejemplo, según lo percibido por la capa de uso, la pérdida del paquete puede siempre no ser cero, el retraso del paquete puede ser variable26. Estos problemas llegan a ser más severos en WMNs debido a su comunicaciones ad hoc y multi-hop. Tales problemas pueden ocasionar fallas en muchos usos del Internet que trabajen suavemente en una red atada con alambre. Actualmente, muchos Protocolos del par-a-par están disponibles para la información que comparte en el Internet. Sin embargo, estos protocolos no pueden alcanzar funcionamiento Satisfactorio en WMNs puesto que WMNs tiene características mucho diversas que el Internet. Desarrollar los usos innovadores para WMNs. Tales usos deben traer enormes ventajas a los usuarios, y también no pueden alcanzar el mejor

funcionamiento sin WMNs. Tales usos permitirán a WMNs ser una solución única del establecimiento de una red.

2.3.2.- SEGURIDAD EN WIRELESS MESH NETWORKS

2.3.2.1.- Descripción de la tecnología en seguridad

Esta sección da una descripción de la tecnología utilizada para la seguridad básica que es necesaria para WMNs. Aquí se hará un resumen general sobre la seguridad en las wireless mesh networks. Las WMN se exponen a las mismas amenazas básicas comunes de las redes alambradas e inalámbricas: los mensajes pueden ser interceptados, modificados, retrasados, reenviado, o los nuevos mensajes pueden ser insertados. Una red que posee recursos importantes, se podría acceder sin autorización.

Los servicios de seguridad que por lo general tratan de combatir estas amenazas son:

• Confidencialidad: Los datos se revelan solamente 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 solamente las acciones autorizadas puedan ser realizadas.

• No negación: Protege las entidades que participan en un intercambio de la comunicación puede negar más adelante algo falso que ocurrió el intercambio.

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

Los Servicios de seguridad en el futuro serán mucho más restringidos buscando para el usuario privacidad (anonimato, seudonimidad, usuario perfilado, y tracing) y la confidencialidad del tráfico.La protección del tráfico de comunicación implica: la confidencialidad (cifrado), la autentificación de los socios de la comunicación, así como la protección de la integridad y de la autenticidad de mensajes intercambiados. La protección de la integridad se refiere no sólo a la integridad del mensaje, sino también al orden correcto de los mensajes relacionados (reenvío, el reordenamiento, o cancelación de mensajes). Esta sección describe la tecnología de protección para el tráfico de la comunicación. Estas tecnologías pueden también ser utilizadas dentro de una red mesh para autenticar los nodos Mesh (MNs) y para establecer las llaves de la sesión que protegen la confidencialidad y la integridad del tráfico intercambiado entre MNs.

El tráfico de la comunicación puede ser protegidas por diversas capas (capa de enlace, capa de red, capa de transporte y capa de aplicación): especialmente en sistemas inalámbricos, (GSM, UMTS, DECT, IEEE 802.11 WLAN, Bluetooth, 802.16 WiMax), que incluye medios de proteger el enlace inalámbrico. Éstos utilizan diversos esquemas de encapsulación de tramas, diversos protocolos de autentificación, y diversos algoritmos criptográficos.

Redes de área local inalámbricas (WLAN) basada en IEEE 802.11i (acceso de Wi-Fi Protected: WPA, WPA2) apoya dos modos de seguridad: también una shared key (llaveo compartida) es configurada en los dispositivos de WLAN (preshared llaveo [PSK]), que es de uso frecuente en las redes caseras, los usuarios pueden ser autenticados con un servidor

autentificador (servidor AAA). Para este propósito, se utiliza el protocolo extensible de autentificación (extensible authentication protocol) (EAP).

La autentificación real ocurre entre la estación móvil (MS) y el servidor AAA Usando EAP (véase Fig II.21). El EAP es transportado entre el MS y el punto de acceso (AP) que usan EAPOL, y entre el AP y el servidor AAA por el protocolo RADIUS. Si es habilitado el nodo, una sesión maestra de llaveo (MSK) es utilizada, el cual se envía desde el servidor de la autentificación (AS) al WLAN AP. Se utiliza como entrada al WLAN

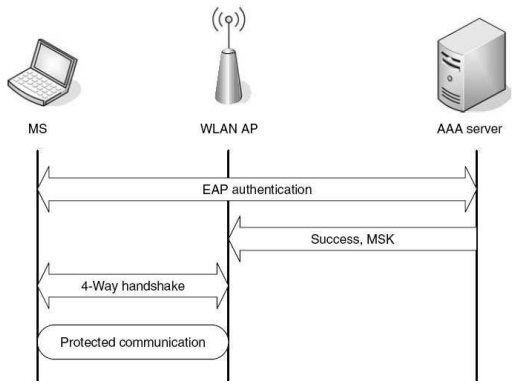

Figura II. 21. Acceso a WLAN basada en EAP

Hay 4 maneras que establece una sesión de llaveo temporal para proteger el enlace inalámbrico. Esta llave se utiliza realmente para proteger el tráfico del usuario, usando cualquier protocolo dominante temporal de la integridad ([TKIP], la parte de WPA) o AES-basado en CCMP (CTR con el protocolo de CBC-MAC, parte de WPA2). Los varios métodos de EAP existen para una autentificación basada en los certificados digitales, las contraseñas, o los protocolos móviles reusing de la autentificación de la red (EAP-SIM, EAP-AKA).

El acceso EAP-basado en WLAN se utiliza particularmente para las redes de la empresa y los hot-spots públicos donde está disponible una base de datos del usuario. El tráfico de la comunicación se puede también proteger en la capa enlace. IPsec protege tráfico IP en la capa de la red (IP). La arquitectura de IPsec especifica dos protocolos de seguridad:

ENCAPSULATION SECURITY PAYLOAD (ESP) y AUTHENTICATION HEADER (AH). En el caso de ESP, ella encapsula solamente la carga útil (payload) del paquete del IP (modo del transporte) o del paquete entero del IP (modo del túnel). Una IPsec security association (SA) define las llaves (keys) y los algoritmos criptográficos para utilizar. Un SA es identificado por 3 cosas consistentes en: un IP address de la destinación, un identificador del protocolo (AH o ESP), y un índice del parámetro de la seguridad.

Este SA unidireccional se puede configurar explícitamente, o puede ser establecido dinámicamente, por ejemplo, por el protocolo del Internet key Exchange (IKEv2). Un uso común de IPsec son las redes privadas virtuales (VPN) para tener acceso con seguridad a un Intranet de la compañía. El tráfico de la comunicación se puede proteger en la capa de transporte usando el protocolo de la seguridad de la capa de transporte (TLS), que se basa en el encendido y es muy similar al secure socket layer (SSL). Su uso principal está para proteger El HTTP sobre TLS/SSL (https), pro esta puede también ser utilizada como protocolo independiente. Los protocolos TLS/SSL28 incluyen la autentificación y el establecimiento del llaveo basado en certificados digitales. Recientemente, la ayuda para preshared o compartir las llaves (PSK-TLS) también fue introducida. Es también posible a

proteger el tráfico en capas más altas. Esto permite para realizar operaciones y aplicaciones específicas de la seguridad. Por ejemplo, los E-mails pueden ser encriptados (protección a la confidencialidad) y/o ser señalados como (autentificación, la integridad, y no compartido del origen) que usa S/MIME o el PGP.

2.3.2.2.- Ediciones de seguridad Mesh

Uno de los objetivos de las WMNs son diversificar las capacidades de redes ad hoc. Las redes ad hoc se pueden considerar realmente como subconjunto De WMNs. Ambas Comparten características comunes, tales como el multihop, wireless, topología dinámica, y membresía dinámica. Por otra parte, las mesh pueden tener infraestructura/backbone wireless y tener menos movilidad. Los esquemas existentes de la seguridad propuestos para las redes ad hoc pueden ser adoptadas para WMNs. Sin embargo, la mayor parte de las soluciones de la seguridad para las redes ad hoc todavía no son bastante maduras para ser puestas en ejecución. Por otra parte, las diversas arquitecturas de red entre WMNs y las redes ad hoc pueden dar una solución para las redes ad hoc ineficaces en WMNs.

Desafíos para la seguridad

Los desafíos para la seguridad de las WMNs se basan en sus características topológicas. Analizando las características de WMNs y comparándolas con otras tecnologías de red, los autores demuestran que los nuevos desafíos de la seguridad son debido a las comunicaciones inalámbricas multihop y por el hecho de que los nodos no están protegidos físicamente.

El Multihopping es imprescindible para que WMNs amplíe la cobertura de redes inalámbricas actuales y proporcionar una non-line-of-sight (NLOS) en la conectividad entre los usuarios. El Multihopping retrasa la detección y el tratamiento de los ataques, hace encaminar un servicio de red crítico, los nodos confían en otros nodos para comunicarse, y la cooperación del nodo es así imprescindible. 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 WMNs son:

• Las WMN puede ser dinámicas debido a cambios en su topología y su membresía (es decir, los nodos entran y salen con frecuencia de la red). Ninguna seguridad con configuración estática sería suficiente.

• En WMNs, los routers mesh y clientes mesh llevan a cabo características muy diversas tales como la movilidad y la energía. Consecuentemente, la misma solución de la seguridad puede no trabajar para ambas al mismo tiempo para mesh router y mesh client.

Descripción de los ataques potenciales a WMNs

Hay dos fuentes de amenazas en las WMNs. Primer, los atacantes externos que no pertenecen a la red mesh pueden atorar la comunicación o inyectar una información errónea. En segundo lugar, amenazas más severas vienen de nodos internos comprometidos, puesto que los ataques internos no son tan fáciles de prevenir como los externos. El ataque puede ser racional, es decir, el adversario no deseado (misbehaves) es bueno para la red solamente si el misbehaving es beneficioso en términos de precio, calidad

obtenida del servicio o ahorro del recurso; si no es indeseado. Los ataques pueden ser distinguidos pasivos y activos. Los ataques pasivos se preponen robar la información y espiar en la comunicación dentro de la red. En ataques activos, el atacante modifica e inyecta paquetes en la red. Además, los ataques podrían apuntar 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 del MAC, un atacante puede abusar de la imparcialidad del acceso medio enviando los paquetes totales del control y de los datos del MAC o personificar un nodo legal. Un atacante podía también explotar los protocolos de la capa de red.Un tipo de ataques es insinuar el conocimiento de los mecanismos de ruteo. Otro tipo es el de packet forwarding, es decir, el atacante puede no cambiar las tablas de ruteo, pero los paquetes en la la trayectoria de encaminamiento puede ser conducida a diferentes destinos que no sea consistente con el protocolo de la encaminamiento. Por otra parte, el atacante puede esconderse en la red, y personificar un nodo legítimo y no sigue las especificaciones requeridas de un protocolo de encaminamiento. En la capa de aplicacion, un atacante podía inyectar una información falsa o imitada, así dañando la integridad de su uso.

Los tipos del ataque se resumen para las redes ad hoc, que están también son aplicables a WMs:

Imitación: La imitación es un ataque en el cual un adversario procura asumir la identidad de un nodo legítimo en la red del acoplamiento. Si los spoofs del adversario legítiman un

Nodo, el adversario pueden tener el acceso a la red para rechazar o recibir los mensajes previstos para nodo spoofed26. Si el adversario spoofs una mesh networks, entonces el Nodo legítima o MNs pueden ser atacados y controlados por el adversario. Considerar el panorama siguiente en el cual un AP comprometido en una red mesh 802.11 finge comportarse normalmente y según los requisitos de 802.11i obtiene las llaves en parejas principales (PMKs) de las estaciones inalámbricas conectadas (WSs).

Normalmente un WS y un AP tienen la opción para depositar el PMK por un período del tiempo. Con esta información, el AP puede engañar fácilmente las WSs y conseguir el *authenticated* usando el PMK almacenado. El AP comprometido puede así aumentar el control sobre este los WS conectándolo con una red del adversario.

Ataque de Sinkhole: Se lanza un ataque del sinkhole cuando una MN malevolo (haber comprometido o adversario que personifica un nodo legítimo) convence nodos vecinos de que sea “lógico” y que tenga salto siguiente para los paquetes de forwarding. El nodo malévolo entonces cae arbitrariamente los paquetes forwarded por nodos vecinos. Este ataque también tiene el potencial de trenzar áreas grandes de la red mesh que son geográficamente distante del nodo malévolo tirando mensajes de sus previstas trayectorias.

Ataque del Wormhole: Un ataque del wormhole procura convencer a nodos que utilicen una trayectoria malévola con medios legítimos. Un adversario con capacidades rápidas de búsqueda puede remitir rápidamente un mensaje con un acoplamiento bajo del estado latente.

Ataque egoísta y codicioso del comportamiento: Un nodo aumenta su poseer la parte del recurso común de la transmisión no pudiendo adherir a los protocolos de red o tratando de forzar con su interfaz inalámbrica.

Ataque de Sybil: En un ataque de Sybil, un nodo malévolo finge identidad de varios nodos, haciendo tan indetectable la eficacia de los esquemas de la fault-tolerace, tales como la redundancia de muchos protocolos de encaminamiento. Los ataques de Sybil también plantean una amenaza significativa a los protocolos geográficos de ruteo. La ruteo enterado de localización requiere a menudo nodos para intercambiar la información coordinada por sus vecinos para encaminar eficientemente los paquetes geográficamente tratados. Usando el ataque de Sybil, un adversario puede actuar adentro más de un lugar al mismo tiempo.

Privación del sueño: Los ataques de privación del sueño son solicitar servicios de cierto nodo, repetidamente, haciendo que el nodo no pueda ir en marcha lenta ni preservando la energía, así privándolo de su sueño y futuro agotando su batería.

DOS y el inundar (Flooding): Los ataques del DOS pueden ser causados por Flooding, es decir, nodos que sobrecargan. Ataques más avanzados del DOS se basan en mensajes de gestión de protocolo inteligente que tratan de forzar. Por ejemplo, los sinkholes son una de las maneras principales de iniciar la expedición selectiva o el nonforwarding de mensajes.

CAPITULO III

IMPLEMENTACION

3.1 Soporte del Sistema Operativo GNU/LINUX para Redes Inalámbricas

Como ya se ha hecho mención, el mercado wireless ha tenido un enorme crecimiento en los últimos años; el cual se atribuye a la gran oferta de productos con esta tecnología, que satisfacen las necesidades de los usuarios. Por tal motivo es necesario introducirse en las capacidades que posee el sistema operativo GNU/Linux para trabajar con las WLAN, las herramientas para proporcionar gestión al tráfico de red, a modo de establecer preferencias, para configurar una tarjeta de red inalámbrica; asimismo como la característica que tiene para clasificar paquetes de acuerdo a ciertas necesidades, la cual es importante para el tema central de este trabajo. Todas estas herramientas se ocuparán

para este proyecto de tesis, debido a las facilidades que ofrece GNU/Linux con respecto a otros sistemas operativos.

3.1.1. Sistema operativo GNU/Linux

GNU/Linux es un sistema operativo de núcleo monolítico el cual fue inicialmente creado como un pasatiempo por un joven estudiante llamado Linus Torvalds, en la Universidad de Helsinki en Finlandia. Linus tuvo un interés en Minix, un pequeño sistema Unix y decidió desarrollar un sistema que excediera los estándares de Minix. Él comenzó su trabajo en 1991 cuando liberó la versión 0.02 y trabajó constantemente hasta 1994 cuando la versión 1.0 del kernel de Linux fue liberada. El kernel, es el corazón de todos los sistemas GNU/Linux, es desarrollado y liberado bajo la licencia GNU General Public Licence, la cual es una licencia que está orientada principalmente a proteger la libre distribución, modificación y uso del software. Asimismo, su código está libremente disponible para quien lo requiera. El kernel es el que forma la base alrededor del cual un sistema operativo GNU/Linux se desarrolla. Actualmente hay cientos de compañías y organizaciones y un igual número de individuos que han liberado sus propias versiones de sistemas operativos basados en el kernel de Linux.

Aparte del hecho de que es libremente distribuido, GNU/Linux es funcional, adaptable y robusto y lo ha hecho la principal alternativa para sistemas propietarios

Durante su segunda década de existencia, ha sido adoptado mundialmente como una plataforma de servidor, esto quiere decir que su mayor aplicación está en convertirse en plataforma para instalar y administrar servicios diversos como páginas Web,

correo, File Transfer Protocolo o FTP, entre muchísimos otros. Su uso como escritorio también está disponible. También está disponible para ser incorporados directamente en microchips y cada vez más está siendo usado en aparatos electrodomésticos y dispositivos. GNU/Linux es usado como sistema operativo en una amplia variedad de plataformas de hardware y computadoras, incluyendo los computadores de escritorio, tales como PCs x86 y x86-64, y Macintosh, servidores, supercomputadoras, mainframes[5], así como también en teléfonos celulares.

La expresión de Linux es utilizada para nombrar a las distribuciones que existen de este sistema, las cuales son diferentes versiones de GNU/Linux que corren variadas aplicaciones pero que contienen el mismo núcleo, también se les conoce como distros o distribuciones.

También tienen diferencias en cuanto a los comandos que ocupan (puede ser el mismo comando pero se escribe de diferente manera) y su intérprete como puede ser bash, ksh, csh, etc. De igual forma hay variación en cuanto a las rutas donde se guardan los archivos de los programas, y de muchas configuraciones. Por ejemplo, un archivo de configuración de un servidor ssh se puede encontrar en la ruta /etc/ssh/sshd.conf en una distribución y en /etc/sshd.conf en alguna otra como Debian.

La distribución que se ocupará para desarrollar este trabajo de investigación será una de las más famosas y utilizadas a nivel mundial Debian.

Debian, es conocido como el sistema operativo universal, viene con 18000 programas pre-compilados que hacen más fácil su instalación. Posee un gestor de paquetes muy intuitivo y fácil debido a que instala dependencias automáticamente.

En este caso, se utilizará la versión Debian Etch (4.0), uno de los sistemas operativos más usados junto con RedHat, es desarrollado por personas voluntarias y se mantiene a base de donaciones de cualquier tipo de personas, aún así es una de las distribuciones más estables y seguras del medio. Sus desarrolladores están comprometidos con la filosofía del software libre descartando llevar paquetes aunque sea con un mínimo aspecto de software privativo e incluyendo sólo software cien por ciento libre, además soporta un total de once arquitecturas de procesador e incluye los entornos KDE, GNOME, igualmente programas criptográficos, es compatible con la versión 2.3 y con aquellos programas desarrollados para la versión 3.1, contiene un proceso de instalación totalmente integrado, con soporte de particiones cifradas, introduce una nueva interfaz gráfica del sistema de instalación que soporta tanto grafías que utilizan caracteres compuestos como lenguas complejas. El sistema de instalación de Debian GNU/Linux ahora está traducido a 58 idiomas.

También se puede decir de Debian que es una de las distribuciones GNU/Linux que se utiliza como base para otras múltiples distribuciones como Knoppix, Linspire, MEPIS, Xandros y la familia Ubuntu, es el más utilizado para implementar servicios de red tales como servidores ssh, servidores web, de correo, entre muchos otros.

Debian es considerado como una de las distribuciones más estables y completas en cuanto a versiones de kernel, repositorios y aplicaciones, fue desarrollado con vista en

administración de servicios y desarrollo y no para usuarios finales. Es por ello que se que se ha elegido esta distribución para el desarrollo de este proyecto.

3.1.2. GNU/Linux y el soporte para redes inalámbricas

Actualmente el sistema operativo GNU/Linux es uno de los más potentes y útiles para el manejo y administración de redes inalámbricas, así como para la administración y configuración de las tarjetas de dichas redes. Desde la configuración de una dirección, hasta controlar el ancho de banda mediante ciertos programas. En fin, es un mundo de posibilidades para las WLAN cuando se utiliza GNU/Linux como plataforma de administración. En esta sección se explicará detalladamente el uso de cada herramienta wireless para mayor información.

Dentro de este contexto se encuentra a una persona que ha sido muy importante en el tema de las redes inalámbricas en su soporte bajo el sistema operativo GNU/Linux, sin importar su distribución: Jean Tourrilhes, quien es el autor del modulo de wireless para Linux que se utilizan para poner a trabajar una tarjeta de red inalámbrica después de que ya haya sido instalado.

3.1.2.1. La extensión wireless

Linux wireless LAN es un proyecto de código abierto (Open Source Project) patrocinado por Hewlett Packard, a través de la contribución de Jean Tourrilhes desde 1996 y es construido con el aporte de muchos usuarios de GNU/Linux alrededor del mundo, con el cual el proyecto va mejorando cada día.

Este proyecto inició cuando Jean Tourrilhes intentó instalar una tarjeta Wavelan en una computadora con GNU/Linux, él tenía dos diferentes versiones del driver para esta tarjeta, uno para la Personal Computer Memory Card International Association o por sus siglas, PCMCIA y otro para la ranura Industry Standard Architecture (ISA) totalmente diferentes con métodos diferentes para instalarlos y debido a que el sistema operativo Microsoft Windows no lo dejó cambiar dichos parámetros optó por modificar el código del driver.

Es por ello que decidió programar una interfaz o API (Application Programming Interface) para las tarjetas inalámbricas, la cual permita a los usuarios manipular cualquier dispositivo de red inalámbrico en una forma estándar y uniforme. Por supuesto, estos dispositivos son fundamentalmente diferentes, así que la estandarización sólo seria en los métodos pero no en los valores.

Esta interfaz debería ser flexible y extensible. La necesidad fundamental fue la configuración de los dispositivos, pero las estadísticas también es deseable. Se necesitó también algo simple de implementar y conforme al estándar de GNU/Linux para tener algo mucho más fácil de compartir y mantener.

La interfaz necesitaría evolucionar con la aparición de nuevos productos y con necesidades específicas. Se intentó ser lo más genérico posible pero Tourrilhes estuvo obligado a restringirse en un conjunto de dispositivos específicos, enfocándose a dispositivos basados en tecnología Wireless LAN. Como sólo fue una extensión al actual interfaz de red de Linux, él decidió llamarla Wireless Extensions o

Extensiones Inalámbricas. Las palabras interfaz y API son también ambiciosas para este simple conjunto de herramientas.

Las Wireless Extensions han sido implementadas en tres partes complementarias. La primera es la interfaz de usuario, un conjunto de herramientas para manipular esas extensiones. La segunda parte es una modificación del kernel de Linux para soportar y definir las extensiones. Y la tercera, es la interfaz del hardware, la cual es implementada en cada driver del nodo para verificar las extensiones a las actuales manipulaciones del hardware. Las modificaciones del kernel han sido incluidas en las versiones 2.0.30 a la 2.1.17. Por defecto, las Wireless Extensions están deshabilitadas cuando una distribución GNU/Linux es instalada. Por lo tanto, se requiere realizar un proceso de recompilación del kernel y habilitar la opción CONFIG_NET_RADIO para el soporte wireless.

Dependiendo de la versión del kernel, el nombre de la opción puede variar.

Las herramientas deben ser capaces de trabajar en cualquier sistema GNU/Linux que haya sido compilado con la opción anterior. Las modificaciones de los drivers es probablemente el reto más importante de los creadores de cada driver. Cada uno necesita soportar las wireless extensions y permitir el correspondiente diálogo con el hardware específico.

La interfaz de usuario está compuesta de tres programas y una entrada /proc en Linux. La ruta /proc/net/wireless es un archivo que da información y estadísticas sobre el

actual sistema inalámbrico. Se despliega en pantalla los siguientes puntos, los cuales son proporcionados por cada dispositivo:

- Status: Su actual estado. Este es una información independiente por cada dispositivo.
- Quality - link: calidad general de recepción.
- Quality - level: fuerza de la señal en el receptor.
- Quality - noise: nivel de silencio (sin paquetes) en el receptor.
- Discarded - nwid: número de paquetes descartados debido al id de la red inválido.
- Discarded - crypt: número de paquetes incapaces de descifrar.
- Discarded - misc: aún no está en uso

Esta información permite tener a los usuarios un mejor panorama del sistema. Así por ejemplo, un alto valor de Discarted – nwid puede indicar que hay un problema de configuración del nwid o que hay una red adyacente. La diferencia entre Quality – link y Quality - level es que la primera indica qué tan buena es la recepción y la segunda qué tan fuerte es la señal. Cuando los valores de Quality han sido actualizados desde la última leída de la entrada, un punto seguirá al valor. Los otros tres programas, forman parte de las herramientas inalámbricas o wireless tools: iwconfig, iwlist e iwspy, detalladas a continuación.

3.1.2.2. Las herramientas wireless

Las herramientas wireless o wireless tools y la extensión wireless (wireless extension) son también proyecto de código abierto patrocinado por Hewlett Packard y desarrollados y mantenidos por la misma persona creadora de las wireless extensions y por la comunidad GNU/Linux. En esta sección se explicarán las herramientas wireless de Linux o mejor conocidas por su nombre el inglés: Wireless tools. Las cuales son un conjunto de herramientas que permiten manipular las Wireless Extensions.

Las wireless tools usan una interfaz textual y son bastante ordinarias para cualquier persona que haya utilizado la línea de comandos de algún sistema GNU/Linux, pero son importantes porque soportan las extensiones completas. A continuación se listan los comandos disponibles y sus posibles parámetros de las wireless tools. Los cuales, como se logra apreciar son amplios y para diversos objetivos.

3.1.2.2.1. iwconfig

Manipula los parámetros básicos de la interfaz inalámbrica. Es un clon de ifconfig, usado para la configuración de dispositivos estándares, como interfaces para redes alambradas. Un ejemplo básico y sencillo del uso de este comando podría ser: iwconfig eth0 essid “una red”, en donde eth0 es el nombre de la interfaz inalámbrica y “una red” es el nombre de la red inalámbrica.

- **ap**: Este parámetro registra el host a un Access Point mediante la dirección MAC.

- **commit**: Aplica los cambios realizados a una interfaz.
- **essid**: Sirve para indicar el nombre de la red a la que se quiere conectar.
- **frag**: Indica el tamaño en que se fragmentarán los paquetes.
- **freq**: Indica la frecuencia de conexión a la que operara el host (k/M/G).
- **channel**: Utilizado para indicar el canal en que actúa o en el que funcionará el dispositivo.
- **key**: Utilizado para indicar la llave en caso de que la red cuente con algún tipo de cifrado.
- **mode**: Utilizado para indicar el modo en que trabajará la tarjeta. Los modos en los que puede operar son: Ad-hoc, Managed, Master, Repeater, Monitor y Secondary.
- **nick**: Sirve para poner un nombre a la estación de trabajo.
- **nwid**: Utilizada para poner un identificador de red. Este parámetro es utilizado sólo por el hardware que funciona con versiones anteriores al 802.11.
- **power**: Para manipular el ahorro de energía.
- **rate**: Define el bitrate o tasa de transferencia a la que funcionará la interfaz.
- **rts**: Agrega una confirmación a un paquete antes de ser enviado, para asegurarse de que el canal en que se está trabajando se encuentre limpio.

- **sens**: Indica la sensibilidad de umbral mínima.
- **txpower**: Define la potencia de envío dBm.

3.1.2.2. 2. Iwlist

Es usado para desplegar alguna información adicional de una interfaz de red inalámbrica, la cual no es desplegada por el comando iwconfig. Permite iniciar el escaneo y listar las redes inalámbricas al alcance, su tasa de transferencia, las llaves, entre muchas otras características.

Cuenta con los siguientes parámetros:

- **ap / peers / access point:** despliega una lista de los Access Point que se encuentran dentro del rango o cobertura. En ocasiones también muestra la calidad del enlace.
- **bit / bitrate / rate:** muestra las tasas de transferencia soportadas por el dispositivo.
- **channel / freq / frequency:** muestra una lista de los canales y la frecuencia a la que puede trabajar cada uno de estos.
- **enc / key / encryption:** muestra los tipos de cifrados soportados y el tamaño de las claves de cifrado.
- **event:** lista de eventos soportados por el dispositivo.

- **power:** muestra los atributos de ahorro de energía que pueden ser utilizados por la interfaz.

- **retry:** muestra el límite de retransmisiones y la duración de las retransmisiones en el dispositivo.

- **scan / scanning:** muestra una listas de la los Access Point o nodos Ad-Hoc a los que se puede conectar el host.

    - **txpower:** muestra la potencia de transmisión de la interfaz.

    - **-versión** muestra la versión de las herramientas, así como la recomendada y actual Wireless Extensions versión de la herramienta y de las distintas interfaces inalámbricas.

3.1.2.2.3. Iwspy

Es usado para establecer una lista de direcciones para monitorear en una interfaz inalámbrica y para obtener por nodo la calidad del enlace y el ruido. Esta información es la misma que la que está disponible en /proc/net/wireless: Calidad del Enlace, Potencia de la Señal y Nivel de Ruido. Esta información es actualizada cada vez que un nuevo paquete es recibido por lo que cada dirección de la lista, añade algo de sobrecarga en el controlador. Esta función sólo opera para los nodos de parte de la célula inalámbrica actual, no puede controlar los puntos de acceso que no están asociadas (se puede utilizar la exploración para eso) ni en los nodos en otras células.

- **lgetthr:** recupera los valores del umbral, definidos por el parámetro setthr.

- **off:** remueve la lista de direcciones definidas por el parámetro setthr y deshabilita esta opción.
- **setthr:** define el límite inferior y superior del umbral.

3.1.2.2.4. Iwpriv

Permite manipular una extensión inalámbrica o wireless específica de un driver. Podría decirse que es una herramienta un tanto experimental. Algunos drivers, como el Wavelan, pueden definir algunos parámetros o funcionalidades extras, iwpriv sd usado para manipularlas. Sin argumentos, iwpriv los comandos privados disponibles en cada interfaz y los parámetros que requiera cada uno. En teoría, la documentación de cada dispositivo debe indicar cómo usar esos comandos específicos para cada dispositivo y sus efectos.

- **--all:** muestra una lista de los comandos privados que no requieren parámetros.
- **roam:** habilita o deshabilita el roaming, si este es soportado por la interfaz.
- **port:** lee y reconfigura el tipo de puerto.

3.1.2.2.5. Ifrename

Permite nombrar interfaces basadas en varios criterios estáticos. Es una herramienta que le permite asignar un nombre coherente a cada una de sus interfaces de red. De forma predeterminada, los nombres de interfaz son dinámicos, y cada interfaz de red se le asigna

el nombre del primero que esté disponible (eth0, eth1). El orden de las interfaces de red al momento de crearse puede variar, para interfaces incorporadas, el orden de arranque del kernel puede variar, para la interfaz extraíbles, el usuario puede enchufar en cualquier orden. De forma predeterminada, cambia el nombre de todos los sistemas actuales definidas en / etc iftab /.

3.1.2.2.6. iwevent

Muestra los eventos generados durante la conexión. Cada línea despliega el evento específico, el cual describe qué ha sucedido en la interfaz inalámbrica específica. Este comando no toma argumentos. Hay dos clases de eventos inalámbricos. El primero de ellos es relacionado a un cambio de configuración en la interfaz (típicamente hecho a través de iwconfig). Sólo son reportadas configuraciones que pueden resultar de una interrupción de conectividad. Todos esos eventos serán generados en todas las interfaces inalámbricas por el subsistema del kernel que soporta esto. La segunda clase de eventos son generados por el hardware cuando algo sucede o una tarea ha sido finalizada.

3.1.2.2.7. iwgetid

Proporciona información sobre la interfaz cuando esta se encuentra conectada. Es usada para encontrar el NWID, ESSID o AP de la red que actualmente está en uso. La información reportada es la misma que la de iwconfig, sólo que iwgetid es más fácil para integrarse en scripts. Por defecto, este comando imprimirá en pantalla el ESSID del dispositivo, y si el dispositivo no tiene algún ESSID, entonces imprimirá su NWID.

- **-a,--ap:** despliega la dirección MAC del Access Point al que se encuentra conectada la interfaz.
- **-c,--channel:** proporciona información sobre el canal actual.
- **-f,--freq:** muestra la frecuencia a la que se encuentra operando la interfaz.
- **-m,--mode:** despliega el modo en que está trabajando la interfaz.
- **-p,--protocol:** muestra el nombre del protocolo que está utilizando la interfaz. Esto permite identificar todas las tarjetas que son compatibles también puede ser utilizado para comprobar Wireless apoyo a la extensión de la interfaz, ya que este es el único atributo que todos los conductores de apoyo Wireless Extensión tienen el mandato de apoyar.

3.1. Pre-requisitos en GNU/Linux

Un driver o controlador es el encargado de actuar como una interfaz entre el sistema operativo (hardware) y los dispositivos que conforman al equipo (Ver figura III.22). Se considera a los drivers como módulos dinámicos que se pueden cargar y descargar cuando se necesite, esto mediante la compilación de un nuevo kernel o recompilación del que se tenga en uso. El kernel de Linux diferencia tres tipos de drivers: drivers de carácter (char devices), drivers de bloque (block devices), drivers de red (network devices).

El objetivo principal de un driver es permitir el acceso a los dispositivos de hardware, sin imponer restricciones arbitrarias a los que usan el driver. En Unix esto

es considerado como una regla de diseño, que se conoce como separación de mecanismos y políticas.

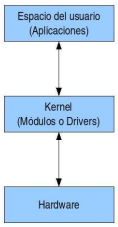

Figura III.22. Interacción Usuario-kernel-hardware

GNU/Linux ofrece una gran cantidad de drivers para varios dispositivos, sin embargo en este trabajo se enfocará en los drivers que ofrece para algunas tarjetas inalámbricas para la creación de WLAN. Una instalación de un driver en GNU/Linux se puede realizar de varias maneras. Dependiendo si el kernel del sistema tiene el soporte necesario para tal dispositivo. En el caso de una tarjeta inalámbrica, el proceso de instalación se hace cuando se compila o recompila el Kernel, el cual se explica a continuación. Es por ello que el primer requisito es un driver y la instalación de una tarjeta inalámbrica en GNU/Linux.

Dentro de los drivers más importantes en GNU/Linux se encuentra Multiband Atheros Driver for Wireless Fidelity o MADWiFi , Aironet, Realtek, Orinoco. Se dice que un driver es considerado software libre si este proporciona el código fuente, ya sea para estudiarlo y entender su funcionamiento o para la modificación del mismo, en caso de ser necesario. El driver sobre el cual se trabajará y abarcará en esta tesis es MADWiFi, el cual funciona bajo el chipset Atheros; este driver soporta la API de wireless extension.

La razón primordial por la cual se decidió utilizar este driver es porque ya se contaba con una tarjeta inalámbrica con un chipset Atheros, soportado por este driver, además de que MADWiFi permite la creación de un punto de acceso. Es distribuido bajo una licencia doble, ya que está basada en las licencias GPL versión 2 y BSD. Considerado como uno de los drivers más avanzados en Linux, es soportado por dispositivos PCI, miniPCI. En lo que respecta a la seguridad MADWiFi permite las siguientes formas de cifrado: WEP, WAP, WAP2.

Una tarjeta inalámbrica puede trabajar en diferentes modos. Un modo es el estado sobre el cual una tarjeta inalámbrica trabaja en una red WLAN y que está limitada a ciertas funcionalidades que el mismo modo ofrece. El más conocido de todos es el modo estación o cliente. Este driver permite ser operado en diferentes modos:

- Access Point (ap): la computadora funciona como un punto de acceso, es decir que los clientes se pueden conectar a los servicios que el access point o punto de acceso ofrece, como puede ser servicio de internet.

- Ad hoc (adhoc): en este modo, la tarjeta se puede conectar con otro cliente directamente para establecer una comunicación punto a punto.

- Estación (sta): la tarjeta wireless se conecta a un punto de acceso con la finalidad de establecer comunicación con otros clientes conectados con el access point mismo.

- Monitor (monitor): Permite capturar paquetes sin tener que conectarse a un AP o a una red ad-hoc.

- wds (wds): este modo permite conectarse con otros puntos de acceso con diferentes fines, tal es el caso de hacer un puente para crear una cobertura de la red más amplia.

Otro requisito ya mencionado arriba es la compilación de un kernel con las opciones necesarias para el soporte de redes inalámbricas. Además, se necesitará soporte para Calidad de Servicio y todos los mecanismos que se derivan de ella y que se explicarán en las siguientes secciones.

3.2. - Instalación de la distribución DEBIAN/ETCH

GNU/Linux se ha desarrollado en muchas variantes, llamadas distribuciones, algunas de las cuales han sido pensadas para solventar necesidades específicas, por ejemplo se encuentran distribuciones con todas las herramientas para implementar seguridades en redes, otras que contienen exclusivamente software educativo, etc.; sin embargo en líneas generales se podría decir que hay dos grandes distribuciones de las cuales se desprenden las demás: DEBIAN y RED HAT/FEDORA.

De estas dos Red Hat se transformó en un sistema de pago y su contraparte Fedora puede ser considerada como la versión de prueba y gratuita. Debian es totalmente libre y gratuito y una de las más reconocidas y apreciadas por la comunidad de software libre por su escalabilidad y robustez.

Para el desarrollo de esta tesis se eligió Debian precisamente por estas características, además del hecho de su filosofía de desarrollo todo el software a instalarse sobre éste puede ser encontrado en fuentes, es decir, el usuario lo puede compilar e instalar según sus necesidades.

El proceso de instalación del sistema operativo se puede desarrollar de dos maneras, ya sea descargando los archivos en formato ISO desde algún repositorio FTP para luego grabarlos en un CD o directamente desde Internet.

Debian se subdivide a su vez en tres versiones: estable, de prueba e inestable, cada una de las cuales recibe un nombre código. Al momento del desarrollo de este trabajo la versión estable se denomina LENNY pero se trabajó con la versión anterior denominada ETCH por su alcance a la misma, la versión de prueba es squeeze y la inestable sid. La versión estable ha sido probada muchos meses antes de ser lanzada y efectivamente suele tener un comportamiento muy robusto, la mayoría de los problemas y bugs han sido solucionados, hay documentación disponible sobre todas sus características e incorpora una gran variedad de software. La versión de prueba en cambio suele tener problemas sobre ciertas plataformas y no tiene la ventaja de correr perfectamente en entornos con configuraciones no comunes o software nuevo. La versión inestable como su nombre lo indica puede generar más de un problema, aunque hay muchos usuarios que lo prefieren pues incorpora las últimas versiones del software disponible.

Se eligió Debian ETCH porque el software necesario para desarrollar esta tesis y el hardware disponible así lo requerían, al inicio se probó con CentOS pero se presentaron

problemas de incompatibilidad entre las versiones del software disponible que se solucionaron con ETCH.

En primer lugar fue necesario descargar desde www.debian.org el primer CD de instalación, luego particionar el disco duro de la PC sobre la que se iba a instalar el sistema operativo y destinar la nueva partición para la raíz del sistema. En principio se eligió una instalación básica, es decir únicamente el sistema base.

Posteriormente se actualizó la base de datos del software disponible con el comando

#apt-dis update

Se modificó el archivo */etc/apt/sources.list* para que contenga:

deb ftp://ftp.debian.org/debian/ testing main

deb-src ftp://ftp.debian.org/debian/ testing main

deb ftp://ftp.es.debian.org/debian/ testing main

deb-src ftp://ftp.es.debian.org/debian/ testing main

deb http://security.debian.org/testing/ update main contrib

Estas son las direcciones web de los repositorios ftp Debian Etch. Con esto se asegura que al actualizar la distribución efectivamente se descarga e instale ETCH, desde el sitio de Debian en los Estados Unidos ftp.debian.org, y si no está disponible, entonces desde el sitio de España ftp.es.debian.org. La última línea hace alusión a un sitio especial, desde donde se descargaran parches de seguridad para el sistema.

Se ejecuta nuevamente apt-dist update y luego apt-dist update, este último comando es el encargado de actualizar la distribución. El proceso en total tardó 2 horas. Al final se consiguió un sistema operativo actualizado y compatible con los requerimientos para este desarrollo.

3.3. Compilación del kernel de Linux

El kernel o núcleo de un sistema operativo es la base sobre cual el software y el hardware se comunican entre sí para poder realizar todas las operaciones básicas de un sistema operativo, siendo realmente como el corazón del sistema, está compuesto por miles de millones de líneas de código, programadas a un bajo nivel, puesto que trabajan con el hardware de una computadora. En cuanto al núcleo de Linux, se puede decir que es de tipo monolítico, es decir, un kernel grande que engloba todas las tareas ya mencionadas en un solo "software". También posee una ventaja muy importante respecto a otros sistemas operativos de tipo privativo o propietarios: es software libre. Esto quiero decir que el código del mismo se encuentra de manera libre para ser descargada y vista por cualquier persona. De igual forma, existe la libertad de distribuir el código y modificarlo sin ningún inconveniente por parte de los desarrolladores. Al contrario, cualquier aportación es recibida de manera positiva por la comunidad GNU/Linux.

Actualmente Linux se encuentra en su versión 2.6.31.12, la cual es la última versión estable, esto quiere decir que se ha probado de errores lo más posible y está lista para su liberación y descarga. Hasta que empezó el desarrollo de la serie 2.6 del núcleo, existieron dos tipos de versiones del núcleo. La versión de producción, es lo que ahora se le conoce

como versión estable. Las versiones de desarrollo se pueden comparar con aplicaciones denominadas betas, o lo que es lo mismo, versiones del kernel que aún no ha sido probadas al cien por ciento o que están en pruebas y se experimenta aún con ellas.

La versión de kernel que etch trae consigo por defecto es la 2.6.18.5. Cada vez que una versión es liberada se agregan nuevas características y como es de esperarse la última versión estable posee nuevos aspectos. Lo que compete, en este caso, son los elementos necesarios para dar soporte de redes inalámbricas.

El proceso de recompilación de un kernel significa en términos generales ajustar un sistema operativo GNU/Linux a la medida mediante una serie de pasos que se explicarán a continuación.

Cabe destacar que el proceso de compilación de kernel en Debian es un poco distinto respecto a otras distribuciones pero no se entrará en detalle acerca de la compilación en otra distribución. Lo primero que hay que hacer es descargar la versión 2.6.23 de la página oficial donde están todas las versiones de los kernel de Linux: http://www.kernel.org/pub/linux/kernel/v2.6/, en formato .tar.gz, ya sea con el comando wget y la URL del kernel a descargar o mediante un navegador Web, específicamente, se necesita descargar el archivo linux-2.6.23.tar.gz.

Ahora se procede a copiar el archivo comprimido dentro del directorio */usr/src/;* esto se logra mediante el comando *cp /ruta/ linux-2.6.23.tar.gz /usr/src/*. Ya estando dentro del directorio especificado, se descomprime utilizando la línea de comandos, de esta forma se escribirá:

tar xvzf linux-2.6.23.tar.gz

Ya descomprimido el archivo, se creará automáticamente un directorio llamado linux-2.6.23, en donde tendrá ya las fuentes del código necesarias para comenzar a compilar.

Ahora, el siguiente paso es instalar algunas aplicaciones que servirán durante este proceso de compilación: *apt-get install kernel-package libncurses5-dev fakeroot build-essential*. Con este comando estamos instalando primero el paquete kernel-package, el cual es utilizado para crear paquetes personalizados del tipo de Debian de un kernel que se haya compilado como se desee. libncurses5-dev es un conjunto de librerías utilizadas para los desarrolladores para escribir interfaces de usuario en terminales independientes. libncurses optimiza la pantalla de cambios, a fin de reducir la latencia experimentada cuando se usan los accesos remotos y algunos otros aspectos relacionados; esta se ocupará para proporcionar un menú de configuración del kernel. El paquete fakeroot funciona para crear paquetes o algunos archivos y darle a los mismos privilegios de superusuario (root) sin tenerlos, de ahí el nombre de fakeroot o falso root. Por último, está el conjunto de paquetes build-essential, los cuales contienen los compiladores de C y C++ necesarios para generar los paquetes de instalación del nuevo kernel a instalar.

Posteriormente se eligen las opciones que con las que el nuevo kernel arrancará cuando se haya compilado. Si se desea se puede hacer una copia del archivo de configuración del kernel en uso para tener una base para continuar configurando. Cuando una distribución Debian se instala, en este caso Etch, con las opciones genéricas de

un kernel, las configuraciones de tal kernel se guardan en el archivo */boot/config-2.6.18-5-486.*

Si se decidió por copiar el archivo a las fuentes del nuevo kernel entonces se escribirá una línea como la siguiente:

server:/usr/src#cp config- 6.18-5-486 ./.config

Después de copiarse esto, ahora se procede a ver el menú de edición de opciones del núcleo, esto se realiza tecleando el comando siguiente y estando siempre dentro del directorio */usr/src/:*

server:/usr/src#make menuconfig

De esta forma saldrá la pantalla principal, la cual se muestra a continuación en la figura III.23

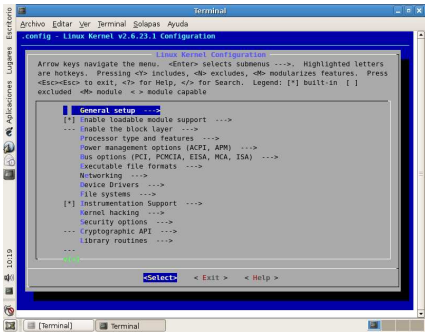

Figura III.23.- Menú principal de configuración del kernel versión 2.6.23

Estando en el menú principal, se cargará el archivo de configuración que se respaldó. Por tanto hay que elegir la opción “Load an Alternate Configuration File”; como

el archivo .config se encuentra en el mismo directorio, no hay que especificar ruta, simplemente el nombre del archivo como se muestra en la figura III.24.

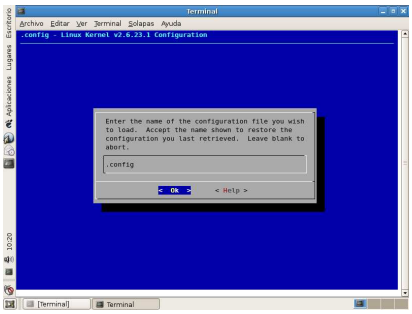

Figura III.24. Cargar un archivo de configuración existente

Antes de compilar, primero hay que escoger las opciones que se requieran para ajustar un kernel a la medida. De esta forma se habilitarán cada una de las opciones como integradas al kernel, lo cual significa que al arrancar el sistema operativo, las opciones estarán listas para utilizarse. Para ello se debe seleccionar la opción a elegir y presionar la tecla “Y”. Así se pondrá un asterisco (*) en la parte izquierda de cada elemento. Si en lugar del asterisco aparece una M quiere decir que el elemento cargará como un módulo del kernel y se tendrá que cargar dinámicamente cada vez que se necesite.

Finalmente, se presiona dos veces seguidas la tecla Esc para salir de este menú.

Aquí se mostrará un diálogo que preguntará si se desea guardar o no guardar la nueva configuración, por lo que se responderá que sí a la pregunta y se dejará el mismo nombre que maneja por defecto: .config, tal como se muestra en la figura III.25.

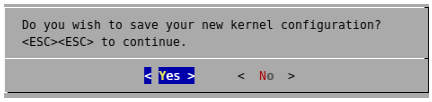

Figura III.25. Diálogo de guardar configuración

El siguiente paso es construir el kernel. Aquí se compilará y construirá el código fuente, generando los paquetes de Debian que se instalarán finalmente. Para compilar las fuentes se debe escribir los siguientes comandos, como siempre, en la línea de comandos:

make-kpkg clean

fakeroot make-kpkg --initrd kernel_image kernel_headers

La opción --initrd crea una imagen initrd en el paquete que se guardará en /boot cuando se instala el kernel. El resultado del comando anterior va a ser crear dos paquetes con extensión .deb en el directorio superior de donde está el código fuente del kernel. Un paquete va a ser el kernel completo y el otro va a ser los kernel-headers o cabeceras. La opción de kernel_headers de la compilación es opcional, pero es recomendable debido a que muchos programas y módulos necesitan tener las cabeceras del kernel que se está usando para poder ser instalados. Este es el caso de MADWiFi. El tiempo de compilación puede variar, dependiendo de la velocidad de procesador que se tenga y de las opciones que se haya habilitado, ya sea como módulos o integrados. Puede realizarse desde media hora hasta dos horas o más.

Una vez que terminó la compilación de los paquetes, se debe subir un nivel en el directorio donde se encuentre. Así, en la ruta /usr/src/ deben existir dos paquetes

con extensión .deb. Para instalar los dos paquetes de Debian generados en el proceso anterior, se utiliza la instrucción dpkg, de esta forma:

dpkg -i linux-image-2.6.23.9_10.00.Custom_i386.deb

dpkg -i linux-headers-2.6.23.9_10.00.Custom_i386.deb

Finalmente, se reinicia la máquina con la instrucción shutdown –r now o init 6 y se selecciona la primer opción del menú de inicio, ya que aparecerá la versión del kernel nuevo, en este caso la 2.6.23.9. De esta forma se finaliza el proceso de re-compilación de un kernel para dar soporte a herramientas inalámbricas.

3.4. Instalación de Wireless Tools

Estas son una serie de suite de herramientas que permiten la comunicación eficiente y rápida del usuario con las distintas opciones de configuración de las tarjetas inalámbricas, estas pensadas precisamente para facilitar las tareas de instalación, configuración y monitoreo de este tipo de dispositivos.

Desde la página oficial de Jean Tourrilhes se descarga el fichero de fuentes wireless_tools.28.pre16.tar.gz. (http://www.hpl.hp.com/personal/Jean_Tourrilhes)

Se ingresa al directorio donde se haya descargado las wireless tools, en este caso bajo usr/src, y se ejecuta la siguiente secuencia de órdenes para descomprimirlo:

debian:#cd /usr/src/

debian:#tar –xzvf wireless_tools.28.pre16.tar.gz

Se crea un nuevo directorio llamado wireless_tools.28.pre16/ en donde se encuentran los ficheros fuente C, se ejecutó el siguiente comando para compilarlos e instalarlos:

debian:/usr/src/#cd wireless_tools.28.pre16

debian:/usr/src/#make

debian:/usr/src/#make install

Se ingresa en el archivo: */etc/ld.so.conf* y se añade la siguiente línea:

/usr/local/lib

Para permitir que el sistema reconozca y ejecute los nuevos comandos.

Por último se ejecuta

debian:#ldconfig

Se verifica el normal funcionamiento con la orden iwconfig; que muestra algo parecido a:

lo no wireless extensions

eth0 no wireless extensions

Es decir el sistema encuentra dos interfaces de red, la de loopback y eth0 o Ethernet, ninguna de las cuales es un adaptador inalámbrico por lo que no soportan wireless extensions, las extensiones del kernel para el manejo de los dispositivos inalámbricos que anteriormente se activaron al compilarlo.

Únicamente cuando wireless tools se hayan compilado e instalado se puede proceder a instalar el driver MADWifi.

3.5. Instalación del Software MADWiFi. (Driver tarjeta inalámbrica)

MADWifi es la contracción de Multiband Atheros Driver for Wifi; driver creado para manipular vía software las tarjetas inalámbricas con chipset Atheros. Este chipset no está soportado nativamente por el kernel de Linux, por lo que es necesario compilarlo e instalarlo.

Atheros es una compañía norteamericana especializada en tecnología inalámbrica que desarrolló este chipset con una propiedad particular: soporta varias bandas de frecuencia simultáneamente y permite crear puntos de acceso para redes inalámbricas. El primer firmware fue desarrollado para la plataforma BSD y luego fue trasladado para la plataforma Linux.

Al momento hay varias generaciones del Chip Atheros, sin embargo las más importantes son:

- 5210 Soporta 802.11a y encriptación WEP vía hardware
- 5211 Soporta 802.11 a y b además de encriptación WEP y AES/OCB vía hardware
- 5212 Soporta 802.11 a, b y g; encriptaciones WEP, TKIP, y AES vía hardware.

El driver se basa en un archivo llamado HAL (Hardware Access Layer, capa de acceso al hardware) que hace las veces de firmware actuando como módulo en el kernel del sistema. HAL se distribuye en un archivo de solo lectura debido a que chipset Atheros puede funcionar fácilmente en frecuencias fuera de las bandas ISM, las mismas que requieren

licencias y por razones de seguridad y reglamentación es preferible suministrar este archivo sin permitir que los usuarios lo puedan manipular. Razón por la cual MADWifi no es un código con licencia GPL ya que HAL es propietario.

HAL está conformado por dos archivos, un binario pre-compilado y ah_osdec.c el cual actúa como intermediario entre el kernel y el binario. Los dos archivos trabajan juntos y forman el módulo kernel ath_hal.ko.

MADWifi depende de dos módulos:

- wlan.ko: Contiene toda la parte de soporte del protocolo 802.11. Esta derivado del primer código incluido en NetBSD y FreeBSD
- ath_hal.ko: Contiene las instrucciones específicas del hardware Atheros.

El driver funciona como un dispositivo normal de red, por lo que está al 100% integrado en el sistema. Hay un solo driver que soporta tanto tarjetas PCI como PCMCIA. Soporta tanto modo máster (Access Point), como modo managed (cliente red inalámbrica con Access Point), y ad-hoc (cliente de red inalámbrica entre iguales); además que es posible poner al adaptador inalámbrico en modo monitor, es decir que actúe como sniffer de una red inalámbrica para detectar y capturar paquetes. Ha sido testeado tanto con kernels 2.4 como 2.6 y requiere extensiones wireless tools posteriores a 14 (kernel 2.4.28 o posterior). Antes de instalarlo y para asegurarse que efectivamente la tarjeta será soportada por MADWifi es recomendable ejecutar lspci, este comando mostrará todos los dispositivos con interfaz PCI conectados en el sistema y arroja un resultado parecido a la figura III.26.

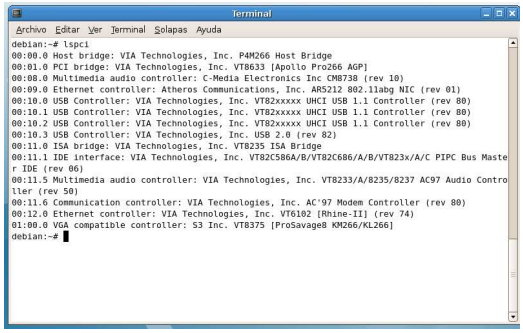

Figura III.26. .- Resultado ejecución lspci en PC con tarjeta inalámbrica instalada

Obsérvese la descripción del cuarto dispositivo encontrado, el sistema detecta que efectivamente se trata de una tarjeta de red (NIC) con chipset Atheros del tipo 5212 que soporta los protocolos a, b y g (es importante anotar aquí que algunos fabricantes cambian el chipset pero sin cambiar la denominación que detectará el sistema, por lo que es muy posible que la tarjeta de trabajo aunque aparente ser Atheros en realidad no lo sea).

Con este resultado se procede entonces a la obtención e instalación del driver. Este se puede obtener desde varios lugares, sin embargo el método más confiable y donde siempre se podrá descargar la última versión es a través de la página oficial del proyecto en www.madwifi.org.

Se mencionarán los pasos a seguir para la instalación de este driver previa re-compilación del kernel, los requisitos necesarios para la instalación son los siguientes:

- Sistema operativo GNU/Linux (Debian Etch).
- Kernel 2.4.x o 2.6.x (Cabeceras y Fuentes).

- Tarjeta inalámbrica con chipset Atheros (En este trabajó se uso una D-Link AirPlus XtremeG Mod. DWL-G520).
- Herramientas de Linux (gcc, make, wireless-tools)
- Fuentes del driver (Se utilizó MADWiFi 0.9.3.3)

Cabe mencionar que el proceso de instalación de una tarjeta inalámbrica en GNU/Linux puede variar dependiendo de la marca de la misma y del driver que se utiliza.

Los pasos para la instalación de MADWiFi son los siguientes:

1. Descomprimir el archivo .tar.gz

debian:/usr/src# tar -xvzf madwifi-0.9.3.3.tar.gz

2. Compilar el driver, al teclear make aparecerá la salida siguiente.

debian:/usr/src /madwifi-0.9.3.3# make

Checking requirements... ok.

Checking kernel configuration... ok.

make -C /lib/modules/2.6.23/build SUBDIRS= debian:/usr/src/madwifi-0.9.3.3 modules

make[1]: Entering directory `/usr/src/linux-2.6.23'

CC [M] /usr/src /madwifi-0.9.3.3/ath/if_ath.o

CC [M] /usr/src /madwifi-0.9.3.3/ath/if_ath_pci.o

LD [M] /usr/src /madwifi-0.9.3.3/ath/ath_pci.o

CC [M] / usr/src /madwifi-0.9.3.3/ath_hal/ah_os.o

HOSTCC / usr/src /madwifi-0.9.3.3/ath_hal/uudecode

UUDECODE / usr/src /madwifi-0.9.3.3/ath_hal/i386-elf.hal.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_hal/ath_hal.o

CC [M] / usr/src /madwifi-0.9.3.3/ath_rate/amrr/amrr.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/amrr/ath_rate_amrr.o

CC [M] / usr/src /madwifi-0.9.3.3/ath_rate/onoe/onoe.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/onoe/ath_rate_onoe.o

CC [M] / usr/src /madwifi-0.9.3.3/ath_rate/sample/sample.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/sample/ath_rate_sample.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/if_media.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_beacon.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_crypto.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_crypto_none.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_input.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_node.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_output.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_power.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_proto.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_scan.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_wireless.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_linux.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_monitor.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_rate.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_acl.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_crypto_ccmp.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_scan_ap.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_scan_sta.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_crypto_tkip.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_crypto_wep.o

CC [M] / usr/src /madwifi-0.9.3.3/net80211/ieee80211_xauth.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_wep.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_tkip.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_ccmp.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_acl.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_xauth.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_sta.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_ap.o

Building modules, stage 2.

MODPOST 13

modules

CC   / usr/src /madwifi-0.9.3.3/ath/ath_pci.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/ath/ath_pci.ko

CC   / usr/src /madwifi-0.9.3.3/ath_hal/ath_hal.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_hal/ath_hal.ko

CC   / usr/src /madwifi-0.9.3.3/ath_rate/amrr/ath_rate_amrr.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/amrr/ath_rate_amrr.ko

CC   / usr/src /madwifi-0.9.3.3/ath_rate/onoe/ath_rate_onoe.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/onoe/ath_rate_onoe.ko

CC   / usr/src /madwifi-0.9.3.3/ath_rate/sample/ath_rate_sample.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/ath_rate/sample/ath_rate_sample.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_acl.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_acl.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_ccmp.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_ccmp.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_ap.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_ap.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_sta.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_scan_sta.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_tkip.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_tkip.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_wep.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_wep.ko

CC   / usr/src /madwifi-0.9.3.3/net80211/wlan_xauth.mod.o

LD [M] / usr/src /madwifi-0.9.3.3/net80211/wlan_xauth.ko

make[1]: Leaving directory `/usr/src/linux-2.6.23'

make -C ./tools all || exit 1

make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/tools'

gcc -o athstats -g -O2 -Wall -I. -I../hal -I.. -I../ath athstats.c

gcc -o 80211stats -g -O2 -Wall -I. -I../hal -I.. 80211stats.c

gcc -o athkey -g -O2 -Wall -I. -I../hal -I.. athkey.c

gcc -o athchans -g -O2 -Wall -I. -I../hal -I.. athchans.c

gcc -o athctrl -g -O2 -Wall -I. -I../hal -I.. athctrl.c

gcc -o athdebug -g -O2 -Wall -I. -I../hal -I.. athdebug.c

gcc -o 80211debug -g -O2 -Wall -I. -I../hal -I.. 80211debug.c

gcc -o wlanconfig -g -O2 -Wall -I. -I../hal -I.. wlanconfig.c

make[1]: Leaving directory `/ usr/src /madwifi-0.9.3.3/tools'

La compilación generará tres ficheros importantes:

- ath_pci.ko (driver para PCI/PCMCIA)
- ath_hal.ko (Atheros HAL)
- wlan.ko (soporte 802.11)

3. Para instalar el driver es necesario tener los privilegios de superusuario (root).

debian:/ usr/src /madwifi-0.9.3.3# make install

```
sh scripts/find-madwifi-modules.sh 2.6.23
for i in ./ath ./ath_hal ./ath_rate ./net80211; do \
        make -C $i install || exit 1; \
    done
make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath'
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
install ath_pci.ko //lib/modules/2.6.23/net
make[1]: Leaving directory `/ usr/src /madwifi-0.9.3.3/ath'
make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath_hal'
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
install ath_hal.ko //lib/modules/2.6.23/net
make[1]: Leaving directory `/ usr/src /madwifi-0.9.3.3/ath_hal'
make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath_rate'
for i in amrr/ onoe/ sample/; do \
        make -C $i install || exit 1; \
    done
make[2]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath_rate/amrr'
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
install ath_rate_amrr.ko //lib/modules/2.6.23/net
make[2]: Leaving directory `/ usr/src /madwifi-0.9.3.3/ath_rate/amrr'
make[2]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath_rate/onoe'
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
install ath_rate_onoe.ko //lib/modules/2.6.23/net
make[2]: Leaving directory `/ usr/src /madwifi-0.9.3.3/ath_rate/onoe'
make[2]: Entering directory `/ usr/src /madwifi-0.9.3.3/ath_rate/sample'
```

```
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
install ath_rate_sample.ko //lib/modules/2.6.23/net
make[2]: Leaving directory `/v/madwifi-0.9.3.3/ath_rate/sample'
make[1]: Leaving directory `/ usr/src /madwifi-0.9.3.3/ath_rate'
make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/net80211'
test -d //lib/modules/2.6.23/net || mkdir -p //lib/modules/2.6.23/net
for i in wlan.o wlan_wep.o wlan_tkip.o wlan_ccmp.o wlan_acl.o wlan_xauth.o wlan_scan_sta.o
wlan_scan_ap.o; do \
        f=`basename $i .o`; \
        install $f.ko //lib/modules/2.6.23/net; \
    done
make[1]: Leaving directory `/ usr/src /madwifi-0.9.3.3/net80211'
(export KMODPATH=/lib/modules/2.6.23/net; /sbin/depmod -ae 2.6.23)
make -C ./tools  install || exit 1
make[1]: Entering directory `/ usr/src /madwifi-0.9.3.3/tools'
install -d /usr/local/bin
for i in athstats 80211stats athkey athchans athctrl athdebug 80211debug wlanconfig; do \
        install $i /usr/local/bin/$i; \
        strip /usr/local/bin/$i; \
    done
install -d /usr/local/man/man8
install -m 0644 man/*.8 /usr/local/man/man8
make[1]: Leaving directory `/usr/src/madwifi-0.9.3.3/tools'
```

4. Ahora lo que se hace es cargar lo módulos del driver MADWiFi al sistema operativo. Después de teclear el modprobe deberá aparecer la nueva interfaz (ath0).

```
debian:/ usr/src /madwifi-0.9.3.3# modprobe ath_pci
debian:/ usr/src /madwifi-0.9.3.3# iwconfig ath0
```

Se ejecuta la orden iwconfig ath0 (las interfaces inalámbricas, para poder diferenciarlas de las interfaces de red Ethernet denominadas ethx suelen denominarse athx, correspondiendo x al número de interfaz usada). Se obtiene una salida parecida a la mostrada en la figura III.27.

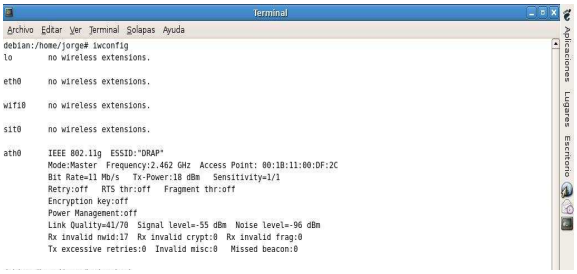

Figura III.27. Resultado de ejecución iwconfig

La pantalla de la figura muestra que se han encontrado tres interfaces de red, eth0 (tarjeta de red Realtek), lo (interfaz de red de loopback) y ath0 (tarjeta de red inalámbrica), donde las dos primeras no soportan las wireless tools y la tarjeta de red ath0 está levantada con la configuración por defecto.

5. Configurar la interfaz inalámbrica, mediante el siguiente comando.

debian:/ usr/src /madwifi-0.9.3.3# iwconfig ath0 essid "NOMBRE DE LA RED" KEY "CONTRASEÑA EN CASO DE TENER" open

Ahora bien, para configurar la interfaz inalámbrica, iwconfig provee los siguientes parámetros (no todos están desarrollados al momento).

3.5.1.- *iwconfig*

interface[essid X] [freq F][channel C] [sens S] [ap A] [rate R]

[rts RT] [frag FT] [txpower T] [enc E] [key K] [retry R]

3.5.2.- essid o Nombre de la red.- Configura el nombre de la red inalámbrica, si se usa en modo managed (cliente de una red inalámbrica de infraestructura) indica la red a la que se conectará la PC del usuario, si se usa en modo máster (punto de acceso).

3.5.3. freq/channel (frecuencia o canal de uso).- Se puede utilizar cualquiera (pero no ambos) de los dos parámetros e indican la frecuencia en la cual funciona el access point o el canal de uso. Si se ingresa un valor entre 1 y 11 el sistema lo interpretara como el canal que se va a usar. Si por contrario se desea configurar una frecuencia de uso entonces se ingresa esta frecuencia en Kilohertz, Megahertz o Gigahertz, siempre y cuando esta sea una frecuencia válida dentro del espectro de las redes inalámbricas.

3.5.4. Sens (Umbral de sensibilidad).- No está implementado en las distribuciones existentes pero se espera que se determine el menor nivel de señal para el cual se recibirán paquetes.

3.5.5. ap (Uso específico de un ap).- Si la interfaz está configurada como managed significa que será cliente de algún punto de acceso, esta opción requiere el ingreso de una dirección MAC del AP al cual se conecta.

3.5.6. rate (Velocidad de transmisión).-Las tarjetas Atheros al soportar diversos protocolos soportarán también distintas velocidades de transmisión: 2 Mbps, 11 Mbps, 54

Mbps, 108 Mbps, etc. Con este parámetro se determina la velocidad teórica máxima a la cual la red inalámbrica trabajará; se digita el valor deseado acompañado de la unidad de medida correspondiente. Es posible utilizar también el modificador *auto* con el cual se permite que sea la interfaz la que determine la mejor velocidad a la cual trabajar.

3.5.7. rts (Umbral rts/cts).- Especifica cuál será la longitud del paquete para el sistema que enviará peticiones rts. Se debe tener cuidado con esta configuración pues puede llegar a ralentizar la red.

3.5.8. frag (Umbral de fragmentación).- Determina la longitud de fragmentación de los paquetes.

3.5.9. key/enc.- Sirven para manipular los distintos tipos de encriptación y niveles de seguridad especificados en el estándar.

Key manipula las claves WEP y los modos de autenticación, enc manipula los tipos de encriptación.

3.5.10. txpower.- Configurará la potencia de transmisión de la interfaz a X dBm. No está implementado.

3.5.11. retry.- Configurará el número máximo de retransmisiones a usarse. No está implementado.

Después de este paso, se está comprobando que la tarjeta está funcionando correctamente en modo cliente y, por consiguiente, fue instalada exitosamente.

3.6. Instalación y configuración de una red mallada

Este capítulo pretende dar una visión del proceso de instalación**,** configuración y utilización de la red. Esta red consta de puntos de acceso inteligentes que son los que se conectan a otra red y permiten a los demás clientes conectarse a ellos. El nodo inteligente consiste en un ordenador personal equipado con dos tarjetas de red inalámbrica. Los ordenadores de esta red están equipados con dos tarjetas inalámbricas la pcmi y otra usb. Una de estas tarjetas, basada en el chipset atheros, está controlada por un *driver* llamado Madwifi que permite utilizar un ordenador como si fuera un AP. Para la red configurada en este proyecto se han utilizado 4 ordenadores que serán configurados como nodos de la red. En la siguiente tabla se pueden ver las características principales de estos nodos, así como los drivers utilizados para sus interfaces Inalámbricas, son 4 ordenadores 2 PCs de sobremesa más dos portátiles

3.6. 1.- Hardware y Software

Tabla III.V. Hadware y Software

Características	Portátil 1	Portátil 2	Sobremesa 1	Sobremesa2
Cpu	Procesador intel core 2 duo 2.20 Ghz	Procesador intel core 2 duo 2.00 Ghz	Pentium IV x386	Pentium IV x386
Memoria	4Ghz	2Ghz	512 Mb	512 Mb
Tarjeta AP	D-Link DWL520	D-Link DWL520	Intel wifi link 5100	Intel wifi link 5100
Driver	Madwifi	Madwifi	Wifi link 5100.gz	Wifi link 5100.gz
Tarjeta ad hoc	D-Link DWA 125	D-Link DWA 125	D-Link DWA 125	D-Link DWA 125
Driver	RT2871 link.tz	RT2871 link.tz	RT2871 link.tz	RT2871 link.tz

3.6.2.- Creación de un Hotspot en GNU/Linux

Un punto de acceso va a ser el modo indicado para este trabajo de tesis por ello lo que prosigue en esta etapa del proyecto es la creación de un Hotspot con la tarjeta inalámbrica que se tiene ya instalada. Un Hotspot es una zona geográfica con cobertura de red WiFi, en donde un access point provee de servicios de red (generalmente servicio de internet) a los clientes conectados dentro de la zona de cobertura de un Hotspot y generalmente se encuentran abiertas, es decir, no requieren de algún tipo de cifrado para poder accederlos, dependiendo de las políticas del lugar.

Se configurará los elementos necesarios para la creación de un Hotspot bajo GNU/Linux. Se necesitará una tarjeta inalámbrica trabajando en modo access point a una velocidad de conexión de 11 o 54 Mbps, al igual que sus clientes. Tal hotspot debe brindar a sus clientes la posibilidad de conectarse a este.

El proceso de creación de un punto de acceso no es del todo complicado. Lo primero que hay que hacer es poner a trabajar a la tarjeta inalámbrica en modo en punto de acceso. Para esto, se utiliza el comando wlanconfig, el cual se encuentra en el directorio tools/ del código fuente del driver MadWiFi y que se instala de forma conjunta cuando el driver mismo se instala en la forma ya especificada. El comando wlanconfig funciona para crear, destruir y manipular interfaces virtuales MADWiFi o Virtual Access Points (VAP); esto quiere decir que principalmente se ocupa para crear interfaces en modo de punto de acceso, pero puede también crear interfaces en modo cliente. Una VAP

es una instancia de una interfaz en modo cliente o punto de acceso y se puede crear más de una interfaz en diferentes modos; para esta finalidad, sólo se ocupará la tarjeta trabajando en un modo particular: punto de acceso.

Las tarjetas inalámbricas instalados con el driver MADWiFi no pueden cambiar su modo de operación con el comando iwconfig, es por ello que se utiliza este comando como herramienta alternativa, de cualquier modo, el resultado es el mismo. Para manejar una interfaz inalámbrica en modo punto de acceso se utiliza los comandos siguientes:

ifconfig ath0 down

wlanconfig ath0 destroy

wlanconfig ath0 create wlandev wifi0 wlanmode ap

El primero de ellos servirá para dar de baja antes que todo, la interfaz que ya se instaló correctamente pero que está funcionando en modo cliente o estación; forzosamente se tiene que darse de baja para poder destruirla. Dar de baja una interfaz es como hacerla inactiva o deshabilitarla, de modo que quede en un estado en el que existe pero no se cuenta con ella para trabajar. El siguiente comando es destruir la interfaz, para que no se libere del sistema operativo y no exista por el momento ningún tipo de interfaz trabajando. Finalmente, se crea la interfaz inalámbrica en modo access point, o modo master, con el tercer comando. Tal comando tiene como parámetros la interfaz inalámbrica, el dispositivo base a través del cual se creará la nueva interfaz y el modo en el cual trabajará, que en esta caso es con las letras ap (access point).

Con estos tres comandos fundamentales, tenemos una interfaz inalámbrica funcionando como punto de acceso. Pero aún falta un elemento fundamental, se

debe asignar una dirección IP, una máscara de red y una dirección de broadcast para que los clientes se conecten, puedan trabajar en la red y accedan a los servicios que prestará esta estación base. La red de esta WLAN pertenece a direcciones privadas, en este caso a la red 192.168.10.0 con una máscara de red por defecto de este tipo de redes de clase C: 255.255.255.0. La dirección de broadcast será la 192.168.10.255. Como es deseable que cada vez que inicie la computadora, tenga ya esa dirección IP fija la interfaz inalámbrica y el modo de trabajo, entonces se procedió a unir el direccionamiento IP junto con la creación de la interfaz en modo master y se colocan ambos en un archivo de configuración muy importante para las interfaces de red bajo GNU/Linux. Este archivo de configuración se encuentra en la ruta */etc/network/interfaces* y contiene todo lo referente a la configuración de cada una de las interfaces existentes en el sistema como direccionamiento IP, la forma de obtener dirección de red, y en este caso la forma de trabajar (master), el canal de comunicación (canal número 2); también se puede observar en el archivo mostrado abajo, que el identificador para el punto de accesso es denominado Mesh.

Después de esto se coloca todos los datos del direccionamiento de la red inalámbrica de área local. Finalmente, otro aspecto relevante de este archivo, es que al final del mismo se colocan las instrucciones para crear la interfaz en modo access point antecedidas por la instrucción pre-up, con lo cual se está diciendo al archivo de configuración que antes que cualquier otra cosa, ejecute esas tres instrucciones. A continuación se muestra el archivo de configuración utilizado para poner a punto la interfaz inalámbrica.

auto lo

iface lo inet loopback

iface eth0 inet static

auto ath0

iface ath0 inet static

wireless-mode master

wireless-channel 11

wireless-essid Mesh

address 192.168.10.2

netmask 255.255.255.0

broadcast 192.168.10.255

pre-up ifconfig ath0 down

pre-up wlanconfig ath0 destroy

pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ap

3.6.3.- Instalación de la tarjeta usb

En nuestros nodos con debían se procede a descargar el driver de la tarjeta D-link DWL 125 para Linux y se procede a descomprimirla de la misma manera que se hizo con la tarjeta pci, luego de un tiempo la tarjeta será reconocida como una interfas ra(0) de esta manera procedemos a configurarla con su dirección ip , Gateway, netmask, network como se muestra en el anexo 1, ya que el procedimiento es parecido a la instalación anterior.

En cuanto a los clientes que están trabajando en Windows Vista se procede a instalarlos con el CD de distribución como se muestra:

Figura III. 28. Asistente de instalación de la tarjeta D-Link DWA 125

Procedemos a instalar el driver como se muestra:

Figura III. 29. Instalación del driver

De esta manera se procede a instalar la tarjeta usb luego de lo cual ya contamos con su perfecto funcionamiento

3.6.4.- Diagrama de funcionamiento

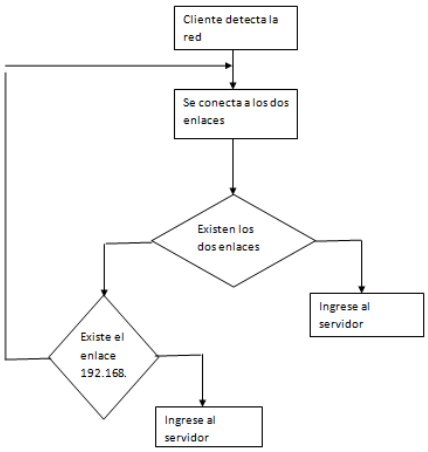

Figura III.30. Diagrama de funcionamiento

3.6.5.- Definición de la red

La red que se desea crear consta de dos tipos de nodos. Los nodos clientes y los nodos AP. Los nodos clientes, son simplemente los usuarios que quieren acceder a la red o a Internet mediante el sistema. En cambio, los nodos AP son los encargados de dar acceso a la red a los clientes y también la señalización entre los distintos nodos APs de la red.

Nodo AP

Un nodo de este tipo debe contar con dos interfaces inalámbricas, una la encargada de dar caracteristicasque se encargará de enviar mensajes de señalización estará en modo ad-hoc para que los APs vecinos tengan la información necesaria que se trata en esta red.

Nodo Cliente

Son equipos equipados con dos tarjetas para enlazarse con cada uno de los enlaces de los nodos mesh para de esta manera cerrar mi red de malla

Una vez que se tiene las interfaces inalámbricas configuradas, los diferentes usuarios se pueden conectar a ellas mediante la red de infraestructura con el ESSID “tesis mesh”. Se debe tener en cuenta que las interfaces deben tener unas IPs de la misma subred que se encuentren estas IPs deben ser del mismo enlace para que los mensajes multicast de señalización lleguen a todos los nodos vecinos.

En la siguiente tabla se puede ver la correspondencia del ordenador físico con el nodo al que se refiere, también se indica la configuración de IPs que se le da a la red:

Tabla III.VI. Direcciones IP

Caracteristicas	**Sobremesa 1**	**Sobremesa 2**
ESSID	Tesis-mesh	Mesh
Direcciones IP	172.30.200.1	192.168.10.2
IP para usb’s	10.10.0.2	10.10.0.1

La conectividad entre los nodos se puede comprobar utilizando un ping hacia alguno de los nodos. Se debe tener en cuenta que sólo se podrán comunicar entre ellos si tienen visibilidad directa y están a una distancia prudencial.

CAPITULO IV

ANÁLISIS Y RESULTADOS

4.1.- Situación actual de la empresa FASTNET Cia Ltda

Fastnet Cia Ltda es una empresa de Telecomunicaciones y Proveedor de Servicios Internet (ISP) para empresas, instituciones, cybers, hogares, etc. Con presencia y cobertura a nivel Nacional. La empresa posee una infraestructura autónoma capaz de proporcionar un servicio de alta calidad adaptándose a las necesidades de sus clientes.

Investigación constante para el desarrollo de nuevos proyectos relacionados al mercado tecnológico.

El segmento de clientes se clasifica en:

- Clientes Home: Son usuarios del hogar.
- Clientes Corporativos: Son usuarios de Centros de Internet (Cybers), Empresas Publicas y Privadas.

La cobertura actual de Fastnet es en Riobamba, Chambo, Licto, Guano, Pungala, Guamote, San Juan, Salinas, La Libertad, San Isidro, Rumicruz y otros sectores dentro del territorio ecuatoriano.

Los equipos usados para enlaces inalámbricos trabajan en las bandas de frecuencias de 2,4 GHz y 5,8 GHz.

Se encuentra estructurada como se muestra en la figura:

Figura Infraestructura de la red FASTNET

4.2.- Analisis de las diferentes aplicaciones que pueden ser usada por FASNET Cia Ltda

Se tiene escenarios conceptuales directamente aplicables a las nuevas WLAN mesh, que se pueden dar uso en la empresa para de esta manera brindar un servicio más eficiente y económico a sus potenciales clientes los cuales se resumen a continuación**:**

ACCESO A INTERNET DE BANDA ANCHA

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

• Coste capital del equipamiento.

• Operación y mantenimiento de un número elevado de nodos.

• Despliegue de cableado en terrenos no urbanizados y de larga distancia.

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

RED MESH COMUNITARIA

Potenciando la idea de mejorar las relaciones entre comunidades vecinas y áreas poblacionales más desfavorecidas a través de la tecnología, algunos ciudades están llevando a cabo proyectos de acceso a Internet de bajo costo, vigilancia contra la delincuencia y redes de información vecinal mediante redes mesh.

En estos escenarios, los participantes son generalmente dueños del equipamiento y de la red mesh y se benefician de la compartición de accesos a través de diferentes tecnologías (cable, xDSL, WxAN…), la redundancia de accesos y el reparto del costo de tarificación.

HOGAR MESH

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

OFICINA INALÁMBRICA

Las redes mesh permiten establecer comunicaciones seguras y eficientes en entornos interiores de oficina, como lo son multitud de comercios. Si cada PC tuviese una tarjeta Wi-Fi mesh se permitiría un despliegue rápido y de bajo coste, eliminando cables, *switches* y puntos de acceso adicionales. Esta opción representa una buena alternativa cuando la inversión en infraestructura cableada resulta demasiado alta (por ejemplo, negocios que dispongan de alrededor de 100 computadoras).

MESH ESPONTÁNEA

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

CAMPUS MESH

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

4.3.- Análisis de la implementación de un plan piloto de una red dentro de un condominio

Consiste en un condiminio que consta de doce departamentos cada uno de sus propietarios tiene la necesidad de acceder a internet. El reto es dotar a estos departamentos de conectividad a redes de información. Frente a este panorama la red que se pretenda aplicar, tiene que ser robusta y sencilla de usar.

La figura muestra la arquitectura que implementaremos para el diseño de la red WMNs.

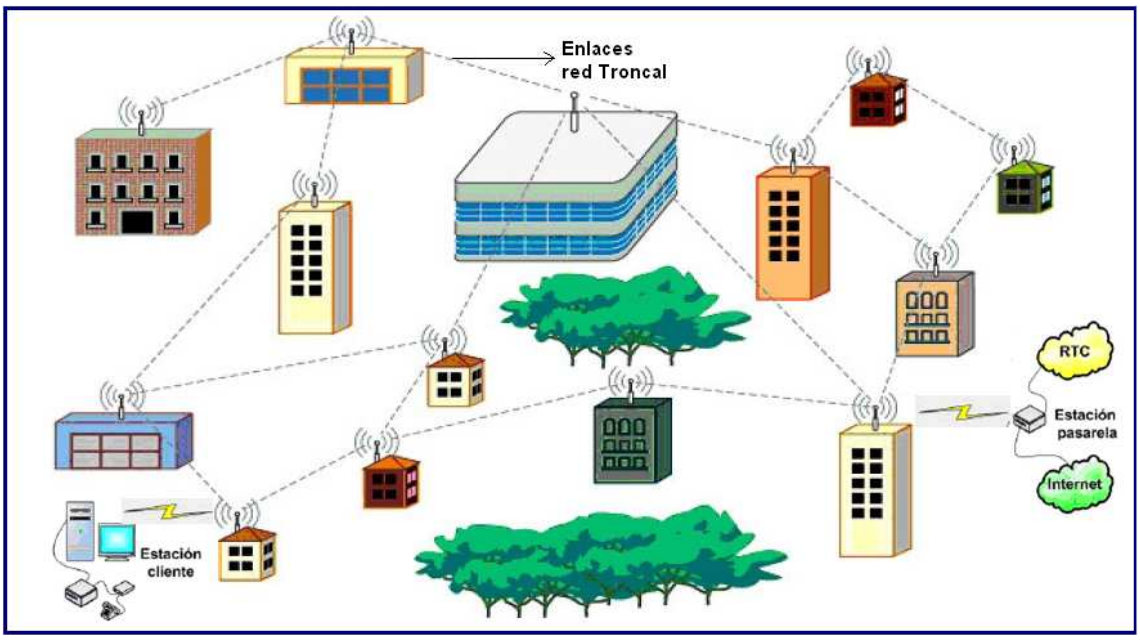

Figura : Arquitectura de red WMNs

Las Redes Inalámbricas Mesh (WMNs) consisten en dos tipos de nodos los repetidores y los clientes, donde los repetidores tienen movilidad mínima y forman la red transporte de la red WMNs. Estás redes pueden integrarse a otras como Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. Los clientes pueden ser estáticos o móviles y pueden crear una red mallada entre ellos mismos o con los repetidores. Estás redes solucionan las limitaciones y mejoran el rendimiento de las redes ad hoc.

Gracias a la posibilidad de conectarse a distintos puntos de acceso en lugar de uno sólo, se aumenta el ancho de banda que puede tener cada cliente, también resulta mucho más estable, ya que puede seguir funcionando aunque caiga un nodo, en cambio en las redes habituales si cae un punto de acceso los usuarios de ese punto de acceso se quedan sin servicio.

En este caso cada uno de los departamentos consta de una PC de escritorio la cual mediante las configuraciones descritas en el capitulo anterior la convertiremos en un nodo mesh de esta manera tendremos un solo nodo conectado a internet y el resto de los nodos podrán acceder sin la necesidad de los molestos cables que aparte de causar molestias dan un mala fachada al edificio de esta manera los clientes ganaran en eficiencia y estética.

Para explicar el funcionamiento de estas redes se a preparado un escenario conformado por cuatro maquinas una vez configurados todos los equipos, es decir, tienen todas las interfaces correctamente configuradas, se está preparado para realizar pruebas de funcionamiento.

4.1.-Prueba de conectividad de la red

En la figura se muestra la estructura de la malla de pruebas

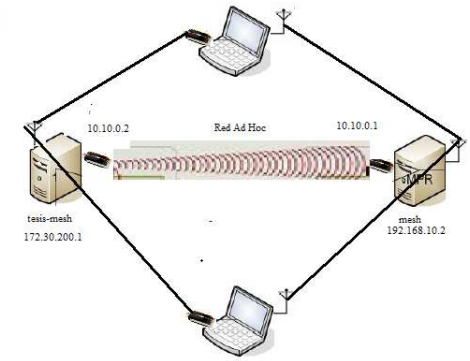

Figura IV.31. Estructura de malla de pruebas

Una vez armada la red procedemos a comprobar la conectividad tanto entre los nodos mesh como con nuestros clientes.

En la siguiente figura mostramos la interface de uno de nuestros clientes en donde le es asignada las direcciones ip para cada una sus interfaces inalámbricas.

```
C:\Users\henrry>ipconfig

Configuración IP de Windows

Adaptador LAN inalámbrico Conexión de red inalámbrica 2:

   Sufijo DNS específico para la conexión. . : drap.org
   Vínculo: dirección IPv6 local. . . : fe80::13:d07f:4e5b:be93x16
   Dirección IPv4. . . . . . . . . . . . . . : 172.30.200.6
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 172.30.200.1

Adaptador LAN inalámbrico Conexión de red inalámbrica:

   Sufijo DNS específico para la conexión. . : drap.org
   Vínculo: dirección IPv6 local. . . : fe80::b9ab:8e99:2365:e22x13
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.10.4
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.10.2
```

Figura IV.32 asignación de ip a las interfaces inalámbricas

Se ha asignado dos direcciones de diferentes redes que corresponden a cada uno de los enlaces que está conectado el cliente las cuales son: 172.30.200.6 la cual pertenece a la red

tesis mesh que se enlaza con la tarjeta usb y la 192.168.10.2 es la dirección que le asigna la red mesh a la tarjeta interna del cliente.

Una vez asignada las direcciones procedemos a realizar las pruebas de conectividad mediante pings:

Figura IV.33 Ping hacia la red mesh que es 192.168.10.2

Figura IV. 34 Ping hacia la interface usb del nodo tesis mesh que es la 10.10.0.2

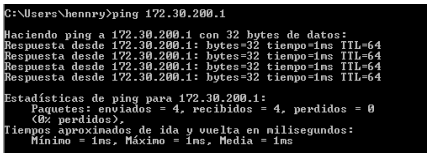

Figura IV. 35. Ping hacia la interfaz pci del nodo tesis mesh que es 172.30.200.1

De esta manera probamos que tenemos conectividad en toda la red

4.2.- Prueba cuando los enlaces se caen

La figura muestra cuando los enlaces de las usb se caen es decir físicamente se desconectan las interface usb.

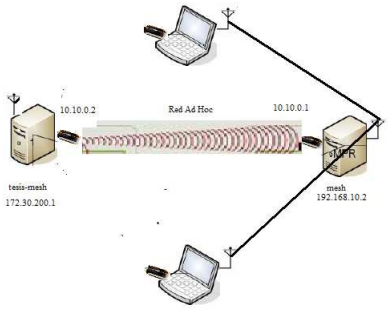

Figura IV.36. Esquema cuando los enlaces se caen

Entonces mediante el programa PuTTY que nos permite un asceso remoto a las pc se comprueba que a pesar de que el enlace directo con el sevidor se ha perdido los clientes podrán seguir ingresando al servidor como se muestra a continuación:

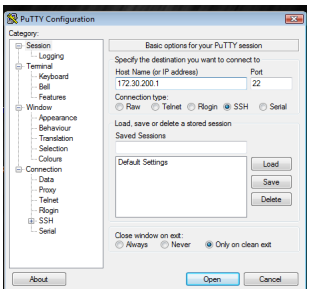

Figura IV. 37. ingreso al servidor 172.30.200.1

Luego del ingreso nos pide la clave y contraseña del servidor con esto se comprueba que el cliente accede al servidor

Figura IV.38. ingreso login y password

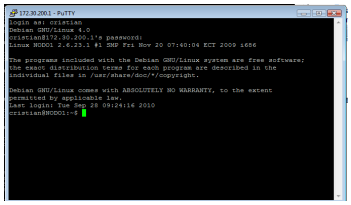

Figura IV.39. Dentro del servidor

Una vez que se ingresa al servidor se procede a realizar un ping hacia nuestra maquina que en este caso es la 192.168.10.4 para comprobar la conectividad en las dos direcciones.

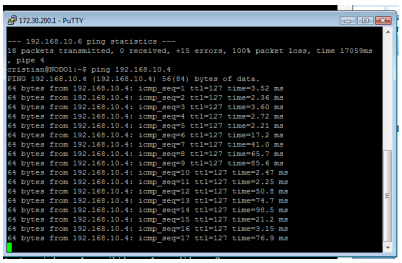

Figura IV.40 ping del servidor hacia el cliente

Además podemos acceder a la página web de la empresa Fastnet Cia Ltda en donde se da una breve descripción de lo que realiza y los servicios que brinda.

Figura IV.41 Página WEb

De esta forma para la implementación de la red piloto en los condominios seria de la misma forma sino que con ocho maquinas más. De esta manera se ha demostrado la funcionalidad de las redes mesh ya que si un enlace se cae siempre habrá otro para poder accesar al servidor de servicios combirtiendole en una red muy robusta.

CONCLUSIONES

1. LAS WMN resultan muy atractivas para la industria y para la sociedad debido a sus bajos costos y a las facilidades de despliegue que poseen, muchos fabricantes, (Tropos, Nortel, Motorola, etc.), los cuales ofrecen hoy en día soluciones muy viables para este tipo de redes.
2. Los grupos de estandarización también se encuentran definiendo nuevas extensiones a las redes inalámbricas para ofrecer funcionamiento enmallado tal como en el caso del 802.11s. Este 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.
3. A nivel técnico, los nuevos retos que suponen estas redes se basan en una estrecha relación entre las distintas capas de pila de protocolos, ya que es necesario optimizar la eficiencia a todos los niveles, siendo difícil si no se tiene información sobre la calidad del enlace para la selección de rutas óptimas. Se podría decir que el diseño de protocolos cross layer es un tópico importante en la investigación actual. Los protocolos usados por las redes Mesh pueden estar basados en topología o en posición, los primeros se encargan de establecer los enlaces entre los nodos dependiendo de la información que se tenga de estos o de la información que aporten los nodos vecinos, en su tabla de enrutamiento; mientras que los segundos establecen el enlace dependiendo de la trayectoria y posición geográfica entre los nodos.

4. El encaminamiento geográfico presenta interesantes características para redes Mesh con un tamaño de moderado a grande. Sin embargo debido a su alto costo, en la actualidad se han empleado protocolos híbridos que combinan los protocolos basados en posición y los basados en topología. Tal y como se a presentado en este documento, se puede comprobar una estrecha relación entre las capas física, Mac y los protocolos de encaminamiento; relación que se acentúa mas al emplear varios canales de radio que requieren de mayor coordinación entre las capas y nuevos mecanismos que se encargan de optimizar el uso del ancho de banda (antenas adaptivas, inteligente, etc.) y minimizar las interferencias.Las redes Mesh presentan varios problemas debido a que han sido diseñadas para uso público. En este momento son muchas las personas que utilizan sus servicios (voz, video y datos) y debido a esto se han hecho grandes cambios en las capas del modelo OSI que contribuyen al mejoramiento de la capacidad, robustez, rendimiento y confiabilidad.
5. Las redes Mesh están apoyadas en la capa física y Mac, sin embargo se están haciendo investigaciones para implementar protocolos en las otras capas. A nivel de la capa física se han creado sistemas Multiantenas y se plantea la incorporación de antenas Mimo (IEEE 802.11n) y las tecnologías de radio OFDM y UWB. En la capa Mac se han dejado atrás los protocolos convencionales como son el aloha y el CSMA, y se incorporan protocolos avanzados como son el RTS y CTS circular, estos protocolos son los encargados de mandarle información a los nodos vecinos para evitar problemas de nodos ocultos, nodos expuestos e interferencias.
6. A nivel de seguridad en la actualidad se están utilizando los protocolos WEP y WPA, los cuales no son muy confiables, y debido a las propiedades de

autodescubrimiento de nuevos nodos y auto-reparación de rutas proporcionada por los protocolos de encaminamiento que utilizan las WMNs, es complejo establecer mecanismos totalmente seguros que permitan autenticar la información recibida, pues si no hay una validación de la información de encaminamiento de los nodos, un atacante malicioso puede comprometer un nodo o introducir un nuevo elemento que puede inyectar a la red información errónea sobre las rutas poniendo en peligro el destino del paquete, empleando diferentes ataque como son la imitación, sybil, wormhole entre otros. Sin embargo se están haciendo investigaciones para decidir si en posible la incorporación del protocolo HTTPS.

7. Con esta tesis se pudo dotar a ordenadores personales, del hardware y software necesario para convertirlos en APs inalámbricas inteligentes, con capacidad para trabajar en las mejores condiciones y con acceso a la red que forman entre todos los nodos.
8. Esta tesis trabajará con tecnologías inalámbricas que cumple todas las normativas exigidas en materia de medio ambiente. Se utiliza la tecnología 802.11b que trabaja en un rango de frecuencias libre (2.4Ghz), por lo que se puede trabajar en él según las leyes vigentes (Ley General de las Telecomunicaciones). Este tipo de redes además de cumplir las normativas tampoco dependen de cableado ninguno por lo que no se deben crear grandes infraestructuras en materia comunicación, aunque sí de electricidad.
9. Con este trabajo se creo una red inalámbrica mallada, en la que todos los nodos que aparezcan puedan trabajar en ella con la mayor calidad posible y sin entorpecer el trabajo de los otros nodos.

-

10. Gracias a la posibilidad de conectarse a distintos puntos de acceso en lugar de uno sólo, se aumenta el ancho de banda que puede tener cada cliente, también resulta mucho más estable ya que puede seguir funcionando aunque caiga un nodo.
11. Hasta que el estándar sea ampliamente adoptado por los fabricantes, podrá cambiar los detalles de las herramientas de configuración. Mientras tanto, si se posee las tarjetas y las herramientas adecuadas, se podrá montar su propia red de malla.

RECOMENDACIONES

1. Se recomienda a FASNET establecer algún software de administración de red con la finalidad de tener un control más riguroso de la red, preferiblemente este software debería ser en sistema operativo Linux para eliminar los costos que se tendrían que pagar por concepto de licencias.
2. Se recomienda aplicar políticas de manejo de la red en caso de ser implementada. Principalmente esta política deberá estar encaminada a entrenar al personal en el manejo de Linux. Ya que este proyecto al ser de carácter social se requiere el máximo ahorro de recursos, e implementado software libre se evitará correr con costos por concepto de licencias, el problema radica en que Linux no es un sistema operativo ampliamente utilizado en el Ecuador por lo que se requiere de capacitación al personal en el manejo de Linux.
3. Se debe implementar Políticas de Seguridad, debido a que la tecnología Mesh permite que un equipo inalámbrico pueda tener acceso a la red sin mayor problema se hace necesario políticas de configuración de los equipos, políticas de acceso remoto, políticas de contraseñas, etc. Que son necesarios para reducir en la medida de lo posible el ingreso a la red de usuario no deseados

RESUMEN

Se implementó un prototipo de red mallada con software libre, para la empresa FASNET Cia Ltda de la ciudad de Riobamba, Provincia Chimborazo, para que FASNET pueda implementar nuevas tecnologías en la empresa. Se empleó métodos lógicos y sintéticos para la unión de los elementos. Empleando GNU/LINUX como sistema operativo en su distribución Debian etch 4.0 sobre dos PC con plataforma x386 de 512 Mb de RAM, Pentium IV, tarjeta de red inalámbrica d-link dwl-g520 air plus y dos usb D-Link dwa 125 se procedió a su instalación compilando el kernel para dar soporte extensiones de administración de redes inalámbricas y de control de tráfico usando MADWIFI y Wireless Tools; para completar la red mallada se utilizo dos laptos cada una con una tarjeta usb y su tarjeta interna para de esta manera se cierre la malla.

De la investigación realizada se determinó que las redes inalámbricas malladas 802.11s son auto configurables, auto reparables y muy seguras. Un aspecto fundamental del funcionamiento de las redes en malla es que la comunicación entre un nodo y cualquier otro puede ir más allá del rango de cobertura de cualquier nodo individual.

Se recomienda a la empresa FASNET Cia Ltda que implemente la red mallada, que brindará a sus clientes servicios eficientes y económicos como para la empresa.

SUMMARY

We implemented a prototype mesh network with free software for the company FASNET Cia Ltda city of Riobamba, Chimborazo Province, to fasnet can implement new technologies in the enterprise. Software was used and synthetic methods for connecting the elements. Using GNU / Linux operating system in Debian etch 4.0 on two PCs running x386 512 MB of RAM, Pentium IV, wireless network card d-link air dwl-g520 usb plus-two D-Link dwa 125 is proceeded to your installation by compiling the kernel extensions to support wireless network management and traffic control using MADWiFi and Wireless Tools; to complete the network mesh is used two laptops each with a usb card and internal card in this way close the net.

In the investigation it was determined that the 802.11s mesh wireless networks are self configurable, self-repairable and very safe. A key aspect of performance of mesh networks is that communication between a node and any other can go beyond the range of coverage of any individual node.

We recommend the company FASNET Cia Ltda that implements the meshed network that will provide customers efficient and economical services to the company.

GLOSARIO

Broadcast: es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Gateway: es una puerta de enlace entre dos redes distintas. Esto significa que se usa como puente, también tiene este significado, entre una red local, LAN, y una extensa, WAN. El significado más empleado actualmente es para designar al dispositivo hardware software o, más usualmente, una combinación de ambos, que controla el tráfico entre Internet y el ordenador o la red local de ordenadores de una empresa.

Multi-Point (Multipunto): tipo de red en la cual cada canal de datos se puede usar para comunicarse con diversos nodos. En una red multipunto solo existe una línea de comunicación cuyo uso esta compartido por todas las terminales en la red. La información fluye de forma bidireccional y es discernible para todas las terminales de la red.

Point-To-Point (punto a punto): tipo de red en las que se usa cada canal de datos para comunicar únicamente a 2 nodos. En una red punto a punto, los dispositivos en red actúan como socios iguales, o pares entre sí.

Wi-Fi (Wireless Fidelity): La expresión que se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que

permite la creación de redes de trabajo sin cables (conocidas como WLAN, *Wireless Local Area Netwoks*).

Beacon.- Señal no direccional transmitida de manera constante por un emisor en una determinada frecuencia cuya misión es informar de su presencia y permitir que los receptores puedan comunicarse con él.

Celda.- Celda en Radiocomunicaciones, define el máximo espacio de cobertura de una estación transmisora dentro del cual todos los usuarios pueden conectarse hacer uso de los servicios que éste brinda.

Paquete.- Cada uno de los bloques en que se divide la información que se envía a través de una red en el nivel de red del modelo OSI. Por debajo de este nivel el paquete adquiere el nombre de trama de red.

-

ANEXOS

ANEXO A

ARCHIVO DE CONFIGURACION DE INTERFACES

/etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static

address 172.30.200.1
netmask 255.255.255.0
network 172.30.200.0
auto ath0
iface ath0 inet static
wireless-mode master
wireless-channel 2
wireless-essid  tesis-mesh
address 192.168.10.2
netmask 255.255.255.0
broadcast 192.168.10.255
pre-up ifconfig ath0 down
pre-up wlanconfig ath0 destroy
pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ap
```

-

ANEXO B

ARCHIVO DE CONFIGURACION DHCP

/etc/dhcpd.conf

```
#Asignación de direcciones de red por DHCP
subnet 172.30.200.0 netmask 255.255.255.0 {
        range 172.30.200.100 172.30.200.110;
        option broadcast-address 172.30.200.255;
        option domain-name-servers 172.30.60.5, 172.30.60.32;
        option routers 172.30.200.1;
}
dhcpd.conf (END)
```

BIBLIOGRAFÍA

1. ARIAS, S.J. Implementación Segura de una red Inalámbrica con Equipo de Recursos Limitados y Herramientas de Software Libre. 2da. ed. Xalapa. México: Depp Multimedia, 2007. 230 p.

2. ENGST, A. y Glenn, F. Introducción a las Redes Inalámbricas. Madrid: Anaya Multimedia, 2003. 180 p.

3. HERBERT, T.F. The Linux TCP/IP Stack: networking qos systems. Hingham: Charles River Media, 2004. 220 p.

4. RAPAAPORT, T.S. Wireless Communications: principles and practice. New York: Prentice Hall, 2002. 200 p.

5. ROBBINS, A. Programación en Linux: casos prácticos. 2da. ed. Madrid: Anaya Multimedia, 2005. pp. 120-145.

Recursos Web

- DEBIAN GNU/LINUX

6. **http://hpl.hp.com/personal/Jean_Tourrilhes/Linux.Wireless.Extensions.htm** (2009-07-10.)

7. http://linux.com/base/ldp/howto/Adv-Routing-HOWTO/index.html
(2010-04-02)

8. http://www.mailxmail.com/curso/informatica/redesbasicas/capitulo4.htm,
(2010-06-13.)

9. http://www.debian.org/
(2010-04-18)

- REDES INALAMBRICAS DE AREA LOCAL

10. http://www.monografias.com/trabajos35/redes-inalambricas/redes
(20010-06-14)

11. http://nmg.upc.es/intranet/qos/9/9.3/9.3.19.pdf
(2010-07-04)

12. http://www.unincca.edu.co/boletin/indice.htm
(2010-08-12)