UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRIA EN TELEMÁTICA

Proyecto Desarrollado previo a la obtención del grado de "Magíster en Telemática"

Diseño e Implementación de un Piloto de Red Wireless para el centro de la ciudad de Loja, basado en Tecnología MESH

JUAN GABRIEL OCHOA ALDEÁN

DIRECTOR: Ing. DIEGO PONCE V. PhD.

CUENCA – ECUADOR

2013

RESUMEN

El avance de las redes inalámbricas en el mundo actual ha permitido que las personas se puedan comunicar sin la necesidad de cables ofreciéndole la libertad de desplazarse sin perder la conectividad, por lo que se vuelva cada día más importante el estudio de soluciones inalámbricas en las ciudades que sirvan para el desarrollo de agendas digitales y permitan el desarrollo de las ciudades, en otras palabras utilizar las tecnologías inalámbricas como herramienta de desarrollo de nuestros pueblos.

Este proyecto desarrollado en el marco de ofrecer a la ciudad de Loja un Piloto de Red Wireless utilizando tecnología mesh tiene como objetivo el conocimiento profundo del protocolo de comunicaciones R.O.B.I.N. (ROuting Batman INside), las configuraciones necesarias en equipamiento de bajo costo y la utilización de software libre en el desarrollo de todo el proyecto.

El presente trabajo plantea en primer lugar el diseño de la red empezando por la selección de un lugar apropiado para su implementación, la selección de equipos, la selección del protocolo de ruteo y documenta paso a paso la implementación del mismo, para al final realizar las pruebas correspondientes a través de analizadores de red y protocolos.

Además el presente trabajo es un primer esfuerzo para crear toda una comunidad virtual que comparta su conectividad a través del portal y equipos de lojasincables.org

Palabras clave: IEEE 802.11, Mesh, Manet, O.L.S.R., B.A.T.M.A.N, R.O.B.I.N.

SUMMARY

The advancement of wireless networks in the world today has allowed people to communicate without the need for wires giving you the freedom to move without losing connectivity, so every day it becomes more important to the study of wireless solutions in cities serving for the development of digital agendas and allow the development of cities, in other words to use wireless technologies as a tool for development of our people.

This project developed in the framework of providing the city of Loja one Wireless Network Driver using mesh technology aims deep knowledge ROBIN communications protocol (Routing Batman INside), the necessary settings on low cost equipment and the use of free software in the development of the entire project.

This paper discusses first the design of the network starting with the selection of a suitable location for deployment, equipment selection, selection of routing protocol and documented step by step implementation of it, to finally make the relevant evidence through network and protocol analyzers.

Furthermore, this work is a first effort to create an entire virtual community to share their connectivity through the portal and equipment lojasincables.org.

INDICE DE CONTENIDOS

CAPITULO I: OBJETIVOS Y MOTIVACION……..10
1. INTRODUCCION……..……10
2. OBJETIVOS……..…10
3. DESCRIPCION DE LOS CAPITULOS……..11
CAPITULO II: MARCO TEORICO……..……12
1. CONCEPTOS GENERALES……12
1.1. Redes Mesh……..……..……12
1.2. Redes Inalámbricas……12
1.3. Clasificación de las redes……12
2. REDES MESH……..……..……..15
2.1. El nivel de enlace……16
2.1.1. IEEE 802.11……17
2.1.1.1. Algoritmo de CSMA/CD……..18
2.2. El nivel de red……..20
2.3. El nivel de transporte……..…..20
2.4. El nivel de aplicación……21
2.5. Tipos de protocolos MESH……..……21
2.5.1. OLSR……..……22
2.5.1.1. Calculo de los MPR's……..25
2.5.2. B.A.T.MA.N……..……..26
2.5.3. R.O.B.I.N……29
2.5.3.1. Características……..…29
2.5.3.2. Nodos ROBIN……30
CAPITULO III: DISEÑO E IMPLEMENTACIÓN DE RED……33
1. DISEÑO……33
1.1. Elección de la ubicación del proyecto piloto……33
1.2. Selección de la conexión a internet……34
1.3. Selección de los equipos y tecnología a utilizar……..35
1.4. Ubicación de los equipos MESH……..……36
1.5. Configuración de Equipos……..36
1.6. Metodos y Herramientas de configuración del FirmWare……38
1.6.1. PUTTY……..38
1.6.2. WinSCP……41
1.7. Herramientas de Monitoreo……42
1.8. Desarrollo del Portal lojasincables……46
1.9. Cálculo de Cobertura Inalámbrica..……50
1.9.1. Método de Trabajo……51
1.9.2. Datos tomados con Netstrumbler……..……52

1.9.3. Datos tomados con EkahauMapper……..……...53
1.9.4. Datos tomados con Wolf Wifi……..…54

CAPITULO IV: PRUEBAS REALIZADAS……..56

1. INSTALACIÓN Y MANEJO DE WIRESHARK…….……56
1.1. Aspectos importantes de Wireshark……..56
1.2. Instalación…..……57
1.3. Prueba realizada…….……58
1.3.1. Filtro paquetes TCP…..……..60
1.3.2. Filtro paquetes UDP……61
1.3.3. Gráfica resumen de la prueba de tráfico……62
2. INSTALACIÓN Y MANEJO DEL JPERF……..63

2.1. Aspectos importantes de Jperf……63

2.2. Instalación……64

2.3. Prueba realizada……..64

3. MECANISMOS DE GESTION DE RED……..…67

3.1. Gestión de red……67

3.2. Gestión de seguridad y acceso a los recursos……67

3.3. Redundancia……69

3.4. Plan de contingencia……..……..69

CAPITULO V: ……..…67

1. CONCLUSIONES Y RECOMENDACIONES……..……78

1.1. Conclusiones……..78

1.2. Recomendaciones……79

BIBLIOGRAFIA…….…… 81

Anexo 1:……..……82

INDICE DE FIGURAS

Figura 2.1. Red Inalámbrica de infraestructura……17

Figura 2.1. Red Inalámbrica Ad-hoc……..18

Figura 2.3. Terminal Oculto y terminal expuesto……19

Figura 2.4. Solución al problema del terminal oculto……..20

Figura 2.5. Formato del paquete OLSR……..23

Figura 2.6. Formato del mensaje MID del protocolo OLSR……..23

Figura 2.7. Formato del mensaje HELLO del protocolo OLSR……..24

Figura 2.8. Formato del mensaje TC del protocolo OLSR……..25

Figura 2.9. Topología de una red con protocolo ROBIN……30

Figura 3.1. Ubicación del proyecto……..36

Figura 3.2. Interfaz gráfica del Putty……..39

Figura 3.3. Interfaz de comandos del Putty……39

Figura 3.4. Interfaz gráfica del WinSCP……..41

Figura 3.5. DashBoard: Configuración General……43

Figura 3.6. DashBoard: Configuración SSID 1……43

Figura 3.7. DashBoard: Configuración SSID 2……44

Figura 3.8. DashBoard: Configuración Avanzada……44

Figura 3.9. DashBoard: Estado de la Red MESH……..45

Figura 3.10. DashBoard: Propiedades del nodo……45

Figura 3.11. DashBoard: Diagrama de Red……..46

Figura 3.12. Portal de acceso a la red MESH……49

Figura 3.13. Lugares de Medición……..52

Figura 3.14. Interface Gráfica del Netstumbler……52

Figura 3.15. Interface Gráfica EkahauHeatMapper……53

Figura 3.16. Aproximación de Cobertura Ekahau……54

Figura 3.17. Interface Gráfica Wolf Wifi……54

Figura 3.18. Diagrama de cobertura inalámbrica de la Red Mesh……55

Figura 4.1. Interfaz Gráfica del Wireshark……..57

Figura 4.2. Muestra de Trafico 1……58

Figura 4.3. Muestra de Trafico 2……58

Figura 4.4. Detalle de paquete UDP……59

Figura 4.5. Detalle de paquete ICMP……59

Figura 4.6. Resumen análisis de tráfico TCP……60

Figura 4.7. ExpertInfo……..61

Figura 4.8. Resumen análisis de tráfico UDP……..61

Figura 4.9. Gráfica resumen análisis de tráfico……...62

Figura 4.10. Interfaz Gráfica del IPERF……64

Figura 4.11. Muestra de tráfico TCP……..65

Figura 4.12. Muestra de tráfico UDP……66

Figura 4.13. Página de acceso a Cloudtrax……67

Figura 4.14. Configuración de Seguridades……68

Figura 4.15. Información de un nodo de la red……68

Figura 4.16. Información de rutas de la red……..69

Figura 4.17. Herramienta de monitoreo de Cloudtrax……75

Figura 4.18. Tasa de transmisión para diversas aplicaciones……..76

Figura 4.19. Canales y frecuencias centrales para 802.11……77

INDICE DE TABLAS

Tabla 2.1. Arquitectura de capas de un nodo manet……15

Tabla 3.1. Ponderación de Lugares……34

Tabla 3.2. Información de nodos……51

Tabla 3.3. Lugares de Medición de RSSI, Ruido, SNR……53

Yo, Juan Gabriel Ochoa Aldeán, autor de la tesis "Diseño e Implementación de un Piloto de Red Wireless para el centro de la ciudad de Loja, basado en Tecnología MESH", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Magister en Telemática. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 01 de julio de 2013

Juan Gabriel Ochoa Aldeán

1103676688

Yo, Juan Gabriel Ochoa Aldeán, autor de la tesis "Diseño e Implementación de un Piloto de Red Wireless para el centro de la ciudad de Loja, basado en Tecnología MESH", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 01 de julio de 2013

Juan Gabriel Ochoa Aldeán

1103676688

CAPITULO I

Objetivos y Motivación

1. INTRODUCCION

El desarrollo de las ciudades siempre ha ido de la mano de la infraestructura que en servicios básicos sus autoridades y en especial los ciudadanos han impulsado e implementado, en un inicio estos servicios fueron el abastecimiento de agua y el desecho de desperdicios y aguas servidas; luego de superado estas necesidades la energía eléctrica y servicio telefónico se convirtieron en necesidades básicas para el desarrollo de las ciudades.

El advenimiento de la sociedad de la información de la mano de avances tecnológicos como el Internet, las Redes Inalámbricas, etc…; ha ocasionado que las necesidades de Telecomunicaciones en las ciudades vayan más allá del servicio telefónico, en otras palabras, el desarrollo de la Red de Redes (World Wide Web), ha cambiado la forma como nos relacionamos en nuestras sociedades, estos cambios se cristalizan cuando la infraestructura de la cual como ciudadanos podamos tener acceso, exista y más importante la infraestructura que como ciudadanos podamos ayudar a construir, en donde se destaca el desarrollo vertiginoso de las TICS, y el esfuerzo de ciudadanos del mundo que crean comunidades virtuales de apoyo en el crecimiento de ciudades digitales.

Las redes inalámbricas han revolucionado los intercambios de datos y definido un nuevo paradigma, el del “Always On-Always Connected", paradigma sobre el cual las comunidades digitales se vienen desarrollando, es por eso que este trabajo es un primer esfuerzo de crear una red mesh piloto en la ciudad de Loja.

2. Objetivos

Objetivo general

- Implementar un Piloto de Red Wireless para la ciudad de Loja, basado en Tecnología MESH.

Objetivos específicos

- Impulsar el desarrollo de redes comunitarias en las ciudades
- Crear una comunidad virtual, a través de un portal lojasincables que permita el desarrollo y crecimiento de la Red.

- Implementar las últimas tendencias en cuanto a redes inalámbricas, en especial aquellas que trabajen con estándares abiertos.
- Contribuir a la reducción de la brecha digital en los países en desarrollo.
- Utilizar en este proyecto piloto el protocolo MESH ROBIN.
- Realizar pruebas del protocolo utilizando la herramienta Wireshark.

3. Descripción de los capítulos

En el capítulo II nos ocuparemos de describir los avances en el campo de las redes MESH, hasta la fecha de hoy. Describiremos los conceptos básicos de las redes mesh y sus características principales, las tecnologías implicadas en su desarrollo y los aspectos a investigar. Nos detendremos con particular atención en describirlos protocolos de encaminamiento que vamos a configurar y probar en el capítulo 4, dado que este tema es el eje central de nuestro proyecto.

En capítulo III se define el diseño de la red, partiendo del escenario en donde se prueba el piloto, el hardware, firmware y software necesarios para la implementación de la Red MESH.

Además este capítulo nos permite conocer los pasos y procesos necesarios para implementación de una red MESH.

Para el capítulo IV se ha definido el software necesario para la realización de las pruebas del protocolo MESH, las mismas que nos permitirán la evaluación del mismo.

Me despido con una serie de conclusiones y recomendaciones finales acerca del trabajo en el capítulo V.

CAPITULO II

Marco Teórico

1. CONCEPTOS GENERALES

1.1. Redes Mesh

Una red MESH (mallada) es aquella en donde cada nodo es conectado directamente a los otros, es decir sin un punto de acceso (AP), lo que permite que la red crezca con la instalación de un nuevo nodo, y además implica que la caída de uno de estos nodos no afecte, en mayor medida, al desempeño de la red.

Denominadas también en algunos artículos como Redes MANET (Mobile ad-hoc Networks), para un estudio más profundo analizaremos las Redes Inalámbricas

1.2. Redes Inalámbricas

Las redes inalámbricas son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Tienen ventajas como la rápida instalación de la red sin la necesidad de usar cableado, permiten la movilidad y tienen menos costos de mantenimiento que una red convencional.

Se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, en donde se ha impuesto un estándar denominado 802.11 del IEEE (Institute of Electrical and ElectronicsEngineers).

1.3. Clasificación de las redes

Por su ámbito:

Wireless Personal Area Network (WPAN).-Red inalámbrica de área personal, incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos celulares, y electrodomésticos) ó un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Se usan varios tipos de tecnología para las WPAN:

Bluetooth, lanzado por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros. La tecnología Bluetooth, también conocida como IEEE 802.15.1, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para usarla en periféricos de pequeño tamaño.

HomeRF, (Home Radio Frequency), lanzada en 1998 por HomeRFWorkingGroup (que incluye a los fabricantes Compaq, HP, Intel, Siemens, Motorola y Microsoft, entre otros) ofrece una velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros sin amplificador. A pesar de estar respaldado por Intel, el estándar HomeRF se abandonó en enero de 2003, en gran medida porque los fabricantes de procesadores empezaron a usar la tecnología Wi-Fi en placa (por medio de la tecnología Centrino, que incluía un microprocesador y un adaptador Wi-Fi en un solo componente).

Zigbee, (también conocida como IEEE 802.15.4) se puede utilizar para conectar dispositivos en forma inalámbrica a un coste muy bajo y con bajo consumo de energía. Resulta particularmente adecuada porque se integra directamente en pequeños aparatos electrónicos (como, por ejemplo, electrodomésticos, sistemas estéreos y juguetes). En principio, el ámbito donde se prevé que esta tecnología cobre más fuerza es en domótica, la razón de ello son diversas características que lo diferencian de otras tecnologías:

- Su bajo consumo.
- Su topología de red en malla.
- Su fácil integración (se pueden fabricar nodos con muy poca electrónica).

El estándar IEEE 802.15.4 define los niveles más bajos: el nivel físico (PHY) y el control de acceso al medio (MAC, parte del nivel de enlace de datos, DLL). El estándar trabaja sobre las bandas ISM. Se definen hasta 16 canales en el rango de 2,4 GHz, cada uno de ellos con un ancho de banda de 5 MHz.

Las radios utilizan un espectro de dispersión de secuencia directa. Se utiliza BPSK en los dos rangos menores de frecuencia, así como un QPSK ortogonal que transmite dos bits por símbolo en la banda de 2,4 GHz. Ésta permite tasas de transmisión en el aire de hasta 250 kbps, mientras que las bandas inferiores se han ampliado con la última revisión a esta tasa desde los 40 kbps de la primera versión. Los rangos de transmisión oscilan entre los 10 y 75 metros, aunque depende bastante del entorno, existiendo aplicaciones en donde se alcanza hasta una milla. La potencia de salida de las radios suele ser de 0 dBm (1 mW).

Wireless Personal Area Network (WLAN).-Red de área local inalámbrica, es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se

encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías:

Wifi (o IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 300 mbps en una distancia de varios cientos de metros.

HiperLAN2 (High Performance Radio LAN 2.0), estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

Wireless Metropolitan Area Network (WLAN).-Red inalámbrica de área metropolitana también se conocen con algunos otros nombres como: bucle local inalámbrico (WLL, Wireless Local Loop), Acceso Inalámbrico de Banda Ancha (BWA, Broadband Wireless Access). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones, pero desarrollado bajo tecnologías propietarias.

WiMAX es un esfuerzo por estandarizar el acceso inalámbrico de banda ancha, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros, en su estándar IEEE 802.16.e.

Por su banda de operación:

Bandas No Licenciadas.- Son redes que operan en las bandas denominadas ISM (Industrial, Scientific and Medical), son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.

Las bandas ISM fueron definidas por la ITU en el artículo 5 de las Regulaciones Radio (RR),

El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida.

Bandas licenciadas.- Son redes que operan en bandas cuyo uso requiere un permiso o título habilitante por parte del organismo regulador de las telecomunicaciones del estado, por lo tanto muchas de las veces su utilización deviene en altos costos.

2. Redes MESH

Una red MESH ó MANET consiste en un conjunto de nodos que se auto-organizan para poder comunicarse entre ellos sin necesitar que intervenga ningún tipo de infraestructura previa desplegada (como pudiera ser una Radio Base de Telefonía Celular o un punto de acceso de una WLAN). Este tipo de redes pueden surgir de forma espontanea y por sus características el medio inalámbrico es el que usan de forma natural para comunicarse.

Los nodos son simultáneamente hosts y routers, ya que pueden tanto ejecutar aplicaciones que hacen uso de la red, como participar en el encaminamiento de los paquetes.

El hecho de usar transmisión inalámbrica influye decididamente en el comportamiento de las manet. Las comunicaciones inalámbricas tienen un rango de transmisión en el que el receptor es capaz de recibir e interpretar correctamente la señal que envió el emisor. Si se encuentra fuera de este rango el receptor no podría interpretar adecuadamente los paquetes que fueron destinados a él. Por eso en las manet los nodos colaboran para enviarse los paquetes de datos enrutándolos salto a salto.

Las manet pueden concebirse como redes aisladas o como extensiones de redes fijas a las que están conectadas. Este último caso es lo que se conoce como redes ad hoc híbridas y necesitan de uno o varios gateways que ejerzan de pasarela entre ambas redes. Hay consenso en el hecho de que las manets no serían redes de tránsito que conecten otras redes, sino que el tráfico estaría originado/dirigido por/hacia los nodos internos.

Arquitectura de un nodo

Nivel de Aplicación	HTTP		FTP
Nivel de Transporte	TCP		UDP
Nivel de Red	IP		
Nivel de Enlace	802.11	BLUETOOTH	WIMAX

Tab. 2.1 Arquitectura en Capas de un nodo manet y los protocolos que se implementas en cada una de ellas

En esta sección mostramos la arquitectura de un nodo que forma parte de una red ad hoc. Al tener las características de host y router simultáneamente su arquitectura es como la que se aprecia en la figura 2.1. Lo más habitual en los nodos de las manet que hemos comentado en esta sección es que implementen la pila de protocolos TCP/IP y que a la vez ejecuten algún

protocolo de ruteo Mesh que probablemente se lanzará como un demonio (demon) que actualizará la tabla de rutas del host.

2.1. El nivel de enlace

Uno de los aspectos más importantes en lo referente al nivel de enlace es el control de acceso al medio (MAC, Medium Access Control). Como las redes inalámbricas utilizan un medio compartido que transporta los datos que emiten ondas electromagnéticas es necesario que los distintos nodos se pongan de acuerdo para no interferir en las comunicaciones de los demás.

Tradicionalmente se han utilizado dos esquemas diferentes para coordinar la comunicación:

Centralizado: Existe un controlador como árbitro que va asignando el turno de palabra a cada uno de los interlocutores. Ningún nodo puede transmitir hasta que le llegue su turno.

Por contienda: No existe ninguna entidad central y por tanto los nodos emiten cuando necesitan hacerlo. En este escenario pueden aparecer colisiones y el protocolo debe ser capaz de recuperarse eficientemente de esta situación.

El carácter descentralizado de las manet hace que el acceso por contienda sea una opción más natural, ya que no se depende de ningún elemento central de coordinación. También resulta más eficiente el no tener que esperar turnos de manera estricta. Aún así los algoritmos centralizados son válidos en cierto ámbito, en especial la de las denominadas WPAN, es el caso de Blueetooh.

Como ejemplo de las tecnologías de nivel de enlace más populares en las redes ad hoc, comentamos a continuación el protocolo IEEE 802.11. Veremos algunos problemas que presentan y cuáles son las vías de investigación que se están explorando.

2.1.1. IEEE 802.11

El estándar IEEE 802.11 ha ocasionado el rápido despliegue y proliferación de las WLANs. El éxito de esta tecnología ha sido rotundo y ha propiciado que la investigación inicial sobre las manet se realice utilizando este protocolo.

802.11 puede operar de dos formas:

Modo Infraestructura.- Las comunicaciones entre dos nodos pasan siempre por un punto de acceso, como en la figura

Fig. 2.1 Red Inalámbrica de Infraestructura

Ad Hoc.- Los nodos se comunican directamente entre sí como en la figura

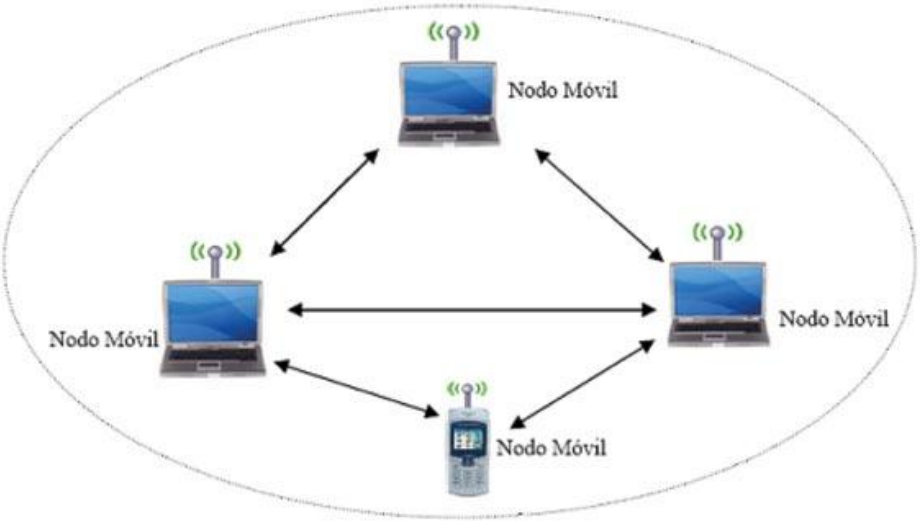


Fig. 2.2Red Inalámbrica Ad-hoc

Esta última forma es la que nos interesa para nuestro trabajo con Redes Manet.

La capa MAC de 802.11 utiliza un acceso por contienda llamado CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) que consiste en que un nodo no transmite si detecta que el canal está siendo usado por otro equipo, y además antes de transmitir se genera un intercambio de mensajes RTS/CTS (Request To Send / Clear To Send) que sirven para que todos los nodos de alrededor se den por enterados de que va a haber una comunicación y cuál es la duración de ésta. Una vez finalizado este periodo los nodos entrarán en contienda por acceder de nuevo al medio.

2.1.1.1. Algoritmo de CSMA/CA

Aunque 802.11 es ampliamente utilizado en el despliegue de manets actualmente, presenta una serie de inconvenientes que degradan el rendimiento que las redes ad hoc alcanzan cuando usan esta tecnología de transmisión. El principal inconveniente es que con alta carga la red se vuelve ineficiente. Uno de los motivos es que el rango de interferencia de cada nodo es bastante grande, por lo que una comunicación puede dañar otra que esté teniendo lugar en una zona lejana de la manet.

Para solventar lo anterior han surgido varias propuestas que intentan adecuar la capa MAC de 802.11 a las redes ad hoc. Una idea consiste en minimizar la potencia con la cual se transmite de forma que la señal llegue lo

suficientemente fuerte al receptor pero afecte al menor número posible de nodos que no están involucrados en la comunicación. Otra línea de actuación consiste en utilizar antenas direccionales de forma que las ondas electromagnéticas sólo viajen en la dirección del destino. Además hay trabajos que propugnan la utilización de múltiples canales (bandas de frecuencias) para permitir que ocurran transmisiones simultáneas de nodos que se encuentran en el mismo rango de cobertura, de forma que no interfieren entre ellas porque las frecuencias utilizadas estarían suficientemente separadas entre sí.

Dos problemas típicos de los esquemas basados en CSMA son la estación oculta y la estación expuesta. En la figura 2.3a vemos como el nodo A transmite hacia el B; como C no se encuentra en el rango de transmisión de A no detecta ninguna comunicación en curso y puede transmitir también hacia el B, provocando una colisión. Otro escenario es el de la figura 2.3b el nodo C transmite hacia D y B quiere hacer lo mismo hacia A. Pero como B escucha el medio ocupado no inicia la transmisión incluso cuando podría hacerlo.

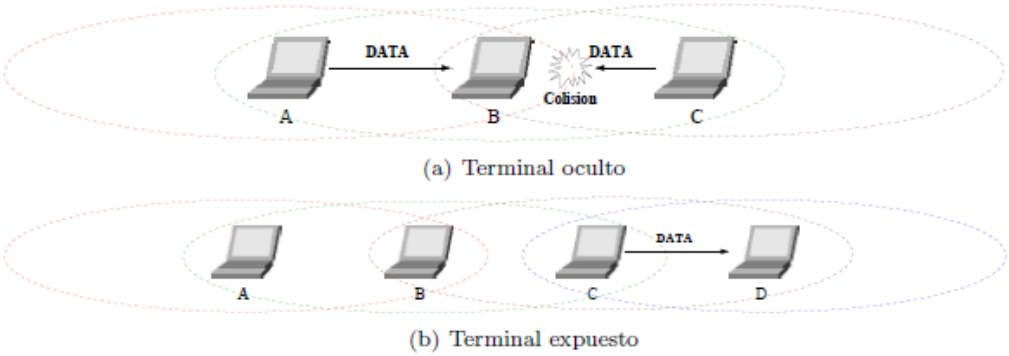


Fig. 2.3 Terminal oculto y terminal expuesto

Para resolver el problema del nodo oculto, IEEE 802.11 articula un sencillo mecanismo (intercambio RTS/CTS) que reserva el medio para una estación (fig. 2.4). El problema del nodo expuesto no se resuelve tan fácilmente y provoca una degradación del rendimiento en las manet basadas en esta tecnología.

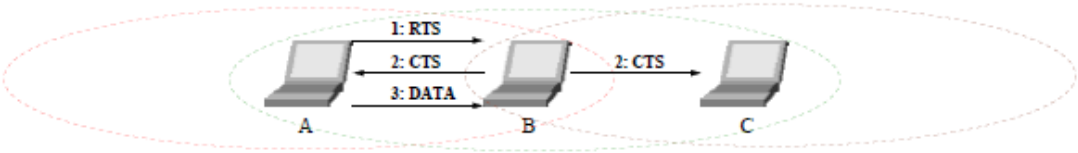


Fig. 2.4Solución al problema del terminal oculto

2.2. El nivel de red

Las redes ad hoc se forman en el nivel de red. Con esto damos a entender que es esta capa la encargada de formar la manet y de enviar los paquetes de datos a sus destinos correctos.

El motivo de hacerlo así es evidente: se consigue que la red ad hoc sea independiente de la tecnología de acceso al medio utilizada. De hecho se puede crear una sola manet cuyos nodos dispongan de diferentes tipos de interfaces y aun así puedan comunicarse entre ellos.

La suite de protocolos en este nivel es la misma que en la pila IP (v4 ó v6). Dichos protocolos pueden sufrir ligeras modificaciones para ser adaptados al entorno de las manet.

Al usar IP como protocolo de red, los nodos de redes ad hoc híbridas pueden comunicarse con el resto de Internet de forma transparente para las aplicaciones.

Como sabemos que cada nodo haría las veces de host y router simultáneamente, es necesario que ejecute algún protocolo de ruteo. Los protocolos de ruteo de las redes fijas (como BGP ó OSPF) no son apropiados en el entorno móvil de las redes ad hoc.

Estudiaremos en detalle estos protocolos en la sección 2.5.

2.3. El nivel de transporte

El protocolo de transporte UDP (User Datagram Protocol).- Ofrece un servicio no confiable y no orientado a conexión de entrega de paquetes.

Esto quiere decir que los mensajes de datos del nivel de aplicación son encapsulados en paquetes UDP y enviados confiando en que llegaran correctamente al destino, pero no se garantiza nada. Son los niveles superiores los encargados de comprobar que todo ha ido bien.

Como UDP es un protocolo tan simple, su aplicación en las manet es directa y no hay ningún inconveniente en utilizarlo.

*El protocolo TCP (Transmission Control Protocol).-*Proporciona un servicio confiable y orientado a la conexión que es mucho más complejo que el de UDP. Este protocolo se definió pensando en las redes cableadas tradicionales y por tanto hace presunciones que no son ciertas en el caso de las redes inalámbricas y por ende tampoco en las manet.

Si en una red fija se pierde un paquete lo más probable es que se deba a la congestión de algún lugar de la red, puesto que el número de errores que aparecen en la transmisión es realmente bajo. En TCP cuando un nodo detecta la pérdida de un paquete asume que se debe a un problema de congestión y reduce la tasa de envío. De esta forma la red se alivia rápidamente y el nodo aumenta de nuevo y paulatinamente la tasa de paquetes que envía.

Pero en las redes inalámbricas hay una tasa de error en las comunicaciones bastante alta y la pérdida de paquetes es común. Además existen otros elementos asociados a la movilidad que hacen que se pierdan paquetes (por ejemplo un mensaje que va destinado a un nodo que momentáneamente se encuentra fuera del rango de cobertura). Sin embargo nos encontramos que en estos casos TCP reduciría la tasa de envío degradando el rendimiento, ya que no es necesario al no haber congestión.

Para obtener un mejor aprovechamiento de TCP en las redes inalámbricas han surgido muchísimas propuestas. La idea básica detrás de todas ellas es dejar intacto el funcionamiento de TCP en la zona cableada (puesto que la buena marcha de Internet depende de ello) y adaptar la parte que se aplica en la red inalámbrica. Estas mejoras se realizan mayormente utilizando proxys que separan la conexión en dos partes, la cableada y la inalámbrica.

2.4. El nivel de aplicación

En este nivel los protocolos empleados serán los mismos a los que ya se utilizan en las redes habituales: DNS, HTTP, POP, IMAP, SMTP), etc; . . .

2.5. Tipos de protocolos MESH

Podemos clasificar los diferentes protocolos de enrutamiento según varios criterios, pero la división más común consiste en distinguir entre protocolos proactivos, reactivos e híbridos.

Proactivos.- Este tipo de algoritmos basa su funcionamiento en tablas, creadas a partir de una fase original de descubrimiento de ruta, que albergan la información referente a los caminos en la red con base a distintos criterios.

Esta información es de ámbito global y por tanto, todos los nodos conservan caminos posibles hacia el resto. Para la diseminación de la misma, los nodos intercambian estos datos periódicamente.

Reactivos.-En este tipo de algoritmos las rutas se construyen únicamente en el momento en que un nodo necesita establecer una comunicación. Es en ese preciso instante cuando se desencadena una fase de descubrimiento de ruta que concluye una vez que la fuente recibe la respuesta del destino que incluye el camino elegido para el envío de datos.

Híbridos.- Este tipo de algoritmos incluye los dos procedimientos anteriores en distintos niveles del enrutamiento. Así, se consigue reducir la sobrecarga de la red con mensajes de control presentada por los algoritmos proactivos, mientras que se disminuye la latencia de las operaciones de búsqueda mostrada entre los reactivos.

2.5.1. Optimized Link State Routing protocol(OLSR)

OLSR tiene como principales características el ser un protocolo de enrutamiento proactivo basado en estado de enlace. Al ser proactivo los nodos que forman parte de la red intercambian periódicamente mensajes de control que permiten aprender la topología de la red. Al estar basado en enrutamiento por estado de enlace dichos mensajes se inundan a toda la red, y la información topológica que contienen consiste en el estado de los enlaces que posee el nodo que originó el mensaje con sus vecinos.

Por ningún motivo, y en especial en redes inalámbricas inundar mensajes en la red es aconsejable además es una operación costosa para los limitados recursos de las redes inalámbricas. El problema se agrava debido a que dicha inundación ocurre de forma periódica.

Para aliviar la situación OLSR utiliza los multipoint relays (MPR) para disminuir la sobrecarga de trafico de control en la red porque sólo los MPR se encargan de retransmitir los mensajes del protocolo de enrutamiento que deben ser inundados.

Para transportar los mensajes de los que hablábamos OLSR define un formato de paquete básico (fig. 2.5) que es entendido por todos los nodos que implementan el protocolo.

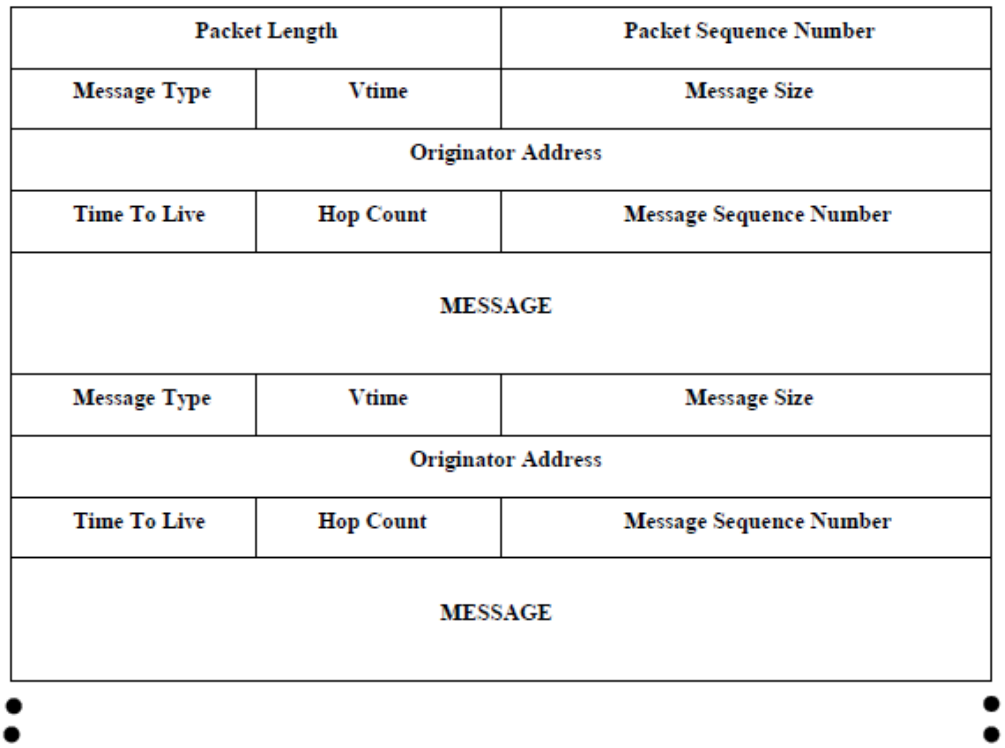


Fig. 2.5Formato del paquete OLSR

Como podemos observar, el paquete puede contener varios mensajes diferentes, y cada uno de esos mensajes puede ser de varios tipos. En la especificación básica de OLSR se definieron tres tipos de mensajes distintos, cada uno para un propósito concreto. Veamos cuales son y porqué se necesitan.

Mensajes MID.-El protocolo tiene soporte para múltiples interfaces en cada nodo, esto es, un mismo nodo puede tener más de una interfaz que está ejecutando OLSR. Por ejemplo, podemos imaginar un ordenador portátil con dos tarjetas WLAN 802.11, o bien una WLAN 802.11 y una WPAN Bluetooth.

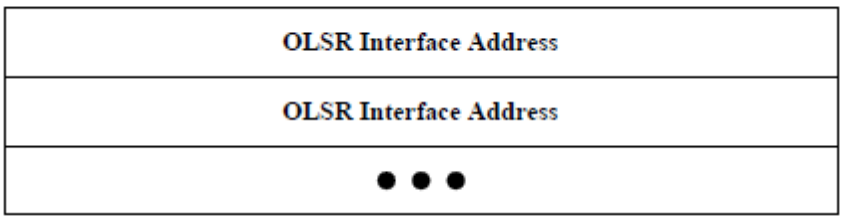


Fig 2.6 Formato del mensaje MID del protocolo OLSR.

Independientemente de la tecnología de acceso a la red empleada ambas interfaces pueden formar parte de la red, cada una con su dirección IP asociada. El resto de nodos deben saber que esas direcciones pertenecen a

interfaces de un mismo nodo, es decir, deben asociar al nodo (dirección IP principal) con el conjunto interfaces (resto de direcciones IP). Esta información es necesaria para calcular correctamente las tablas de enrutamiento.

Por lo anterior en OLSR cada nodo que posea múltiples interfaces participando de la red debe anunciar periódicamente las direcciones de éstas mediante mensajes MID

Los mensajes MID se transportan por toda la red haciendo uso del mecanismo de inundación optimizado que proporcionan los MPR.

Mensajes HELLO.- Los nodos de la red deben conocer los enlaces que tienen con los nodos vecinos y cuáles el estado (unidireccional, bidireccional o roto) de dichos enlaces. Además para que un nodo pueda seleccionar su conjunto de MPR´s necesita conocer cuáles son sus vecinos y cuáles son los vecinos que tiene a dos saltos. Cuando ya ha calculado el conjunto de nodos que serán sus MPRs debe notificarlo a dichos nodos de alguna forma.

Realizar las tareas anteriores se conoce como “descubrimiento de la topología local” y en OLSR es llevado a cabo mediante el intercambio de mensajes HELLO (figura 2.7).

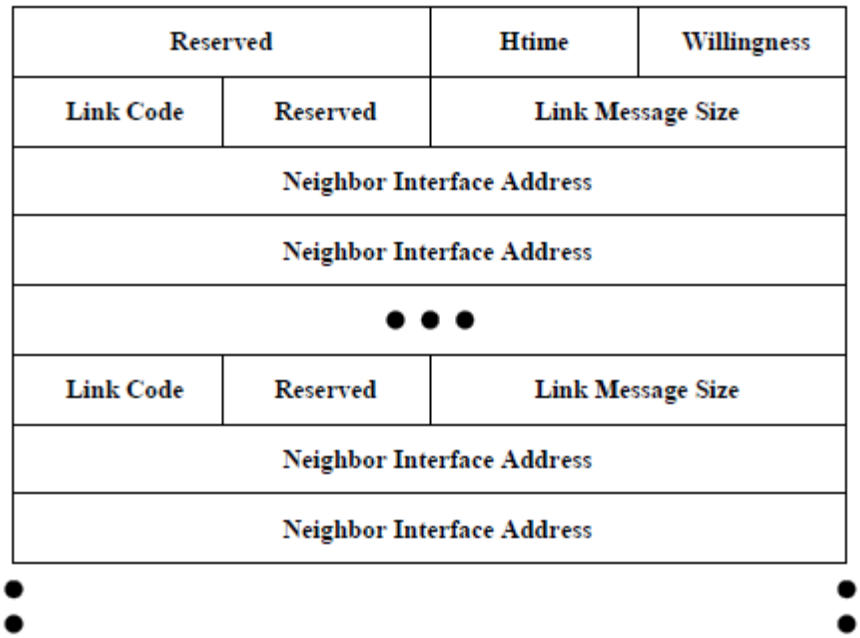


Figura 2.7. Formato del mensaje HELLO del protocolo OLSR.

Dichos mensajes sólo viajan hasta el vecindario inmediato de un nodo, por lo tanto nunca son retransmitidos.

Mensajes TC.-Utilizando los mensajes anteriores un nodo ya conoce los enlaces que tiene con sus vecinos y el estado de los mismos, así como la información necesaria para aplicar el mecanismo de los MPR. Ahora hay que aprovecharlo para diseminar la información topológica de estado de enlace.

En el protocolo de estado de enlace clásico, cada nodo genera mensajes de información topológica en los que anuncia los enlaces que tiene con todos sus vecinos. OLSR minimiza el número de dichos mensajes ya que sólo serán generados por los MPR. Además se minimiza también el tamaño de esos mismos mensajes porque los nodos pueden anunciar sólo información parcial acerca de la topología de la red y aun así OLSR todavía sería capaz de proporcionar rutas óptimas en cuanto al número de saltos. Dicha información que como mínimo debe anunciar un nodo consiste en los enlaces que existen entre él y aquellos vecinos que lo han seleccionado como MPR. Con todas estas optimizaciones OLSR se convierte en un protocolo apto para ser utilizado en redes densas ya que así se le puede sacar mayor partido al uso de los MPR.

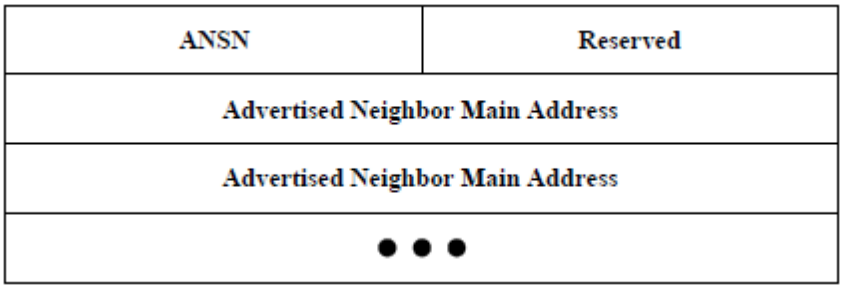


Figura 2.8. Formato del mensaje TC del protocolo OLSR.

Por tanto, los nodos que hayan sido seleccionados como MPR por algunos vecinos generarán periódicamente mensajes de tipo TC donde anunciarán, al menos, los enlaces que tienen con dichos vecinos (ver fig. 2.8). Estos mensajes se diseminarán por toda la red gracias a los MPR, proporcionando así la información necesaria para calcular rutas hacia cada nodo de la red.

2.5.1.1. Cálculo de los MPR´s

Los MPR´s son calculados de modo que un nodo puede llegar a todos sus vecinos ubicados a una distancia de dos saltos a través de uno de estos MPR.

La técnica de los MPR está diseñada para reducir el número de retransmisiones redundantes que tienen lugar por parte de los nodos de la red.

El mecanismo MPR se basa en reducir el conjunto de nodos de la red que van a retransmitirlos mensajes broadcast, de tal forma que el mensaje llegue a

todos los nodos de la red con el menor número de retransmisiones. Cada nodo va a calcular cuál es ese conjunto mínimo de vecinos que deben retransmitir sus mensajes de control, y sólo ellos efectuarán las retransmisiones. Dicho conjunto mínimo es lo que se conoce con el nombre de multipoint relays (MPR), y se calcula averiguando el menor número de vecinos que se necesitan para alcanzar a todos los nodos que se encuentran a dos saltos de distancia.

Para averiguar el conjunto de MPRs es necesario intercambiar previamente cierta información acerca de la topología "local" de la red.

2.5.2. Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.)

El problema con los clásicos protocolos de enrutamiento es que son por lo general no muy adecuados para las redes inalámbricas ad hoc. Esto se debe a que estas redes no tienen estructura, dinámica, cambia su topología, y se basan en un medio inherentemente poco fiables.

OLSR, el protocolo más empleado actualmente para tales escenarios, ha sufrido una serie de cambios con la configuración original con el fin de hacer frente a los desafíos impuestos por las redes mesh. Mientras que algunos de sus componentes demostraron ser inadecuados en la práctica (como el MPR e Histéresis) nuevos mecanismos se han añadido (como Ojo de Pez y ETX). Sin embargo, debido al constante crecimiento de las redes de malla y debido a la exigencia inherente de un algoritmo de estado de enlace para volver a calcular la topología de todo el gráfico (una tarea particularmente difícil para la reducida capacidad del router), los límites de este algoritmo se han convertido en un reto.

El enfoque del algoritmo BATMAN es dividir el conocimiento sobre las mejores rutas de extremo a extremo entre los nodos de la malla a todos los nodos participantes. Cada nodo percibe y mantiene sólo la información sobre el mejor próximo salto hacia todos los demás nodos.

De esta manera la necesidad de un conocimiento global sobre los cambios de topología local se convierte en innecesario. Además, un evento basado pero intemporal (eterno en el sentido de que Batman nunca horarios ni información tiempos de espera de topología para optimizar es decisiones de enrutamiento) inundaciones mecanismo evita que el devengo de contradecir información de la topología (la razón habitual para la existencia de bucles de enrutamiento) y los límites cantidad de mensajes que inundan el topología de malla (evitando así la excesiva sobrecarga de control de tráfico). El algoritmo está diseñado para hacer frente a las redes que se basan en los enlaces poco fiables.

El algoritmo de protocolo de Batman se puede describir (simplificado) de la siguiente manera:

Cada nodo transmite mensajes de difusión (OGMs) para informar a los nodos vecinos acerca de su existencia.

Estos vecinos se vuelven a transmitir mensajes OGMs de acuerdo a normas específicas para informar a sus vecinos acerca de la existencia del iniciador original de este mensaje y así sucesivamente y así sucesivamente.

Así, la red está inundada de mensajes de autor. Los OGMs son pequeños, el tamaño típico del paquete es de 52 bytes incluyendo overhead IP y UDP. Los OGMs contienen por lo menos la dirección del originador, la dirección del nodo que transmite el paquete, TTL y un número de secuencia.

Los OGMs que sigan un camino donde la calidad de los enlaces inalámbricos sea pobre o los enlaces estén saturados sufrirán de pérdida de paquetes o retraso en su camino a través de la malla. Por lo que, los OGMs que viajan en rutas buenas se propagan de manera más rápida y confiable.

Con el fin de saber si un OGM se ha recibido una o más de una vez, cada OGM contiene un número de secuencia, asignada por el nodo originador del OGM. Cada nodo re-envia los OGMs recibidos en más de una vez y sólo los recibidos desde el vecino que ha sido identificado como el actual siguiente mejor salto (vecino mejor rankeado) hacia el iniciador original de los OGM.

De esta manera los OGMs se inundan de forma selectiva a través de la malla e informan a los nodos receptores sobre la existencia de otro nodo. Un nodo X aprenderá acerca de la existencia de un nodo Y en la distancia, al recibir sus OGMs, cuando los OGMs del nodo Y son reenviados por sus vecinos de un solo salto. Si el nodo X tiene más de un vecino, puede decir por el número de mensajes emisores que recibe, la vía más rápida y fiable a través de uno de sus vecinos de un solo salto, qué vecino tiene que escoger para enviar los datos al nodo distante. El algoritmo entonces selecciona este vecino como el actual mejor salto junto al creador del mensaje y configura su tabla de enrutamiento, respectivamente.

Historia

La tarea consistía en crear un protocolo que fuera tan fácil, tan pequeño y tan rápido como sea posible. Parece por tanto razonable dividir el desarrollo en varias fases e implementar funciones complejas mediante un proceso iterativo:

Versión uno

En la primera fase, el algoritmo de enrutamiento fue implementado y probado por su practicidad e idoneidad para la tarea en cuestión. Para el envío y

recepción de mensajes de origen (información acerca de la existencia) fue escogido el puerto UDP 1966.

Versión dos

En esta versión se realiza en el algoritmo una suposición importante: tan pronto como un nodo recibe datos existencia de otro nodo, se supone que también puede enviar datos de regreso. En las redes de radio, sin embargo, puede muy bien ser factible que la comunicación se realice en un solo sentido. Un mecanismo fue incorporado en el protocolo para permitir esto y para resolver los problemas planteados. El mecanismo permite que el nodo determine si un nodo vecino proporciona una comunicación bidireccional, sólo los nodos bidireccionales se consideran parte de la red, los nodos de una vía no son completamente incluidos.

Versión tres

La mayor innovación de esta versión es el soporte B.A.T.M.A.N. de los dispositivos de red múltiples. Ahora, un ordenador o un router ejecutando B.A.T.M.A.N. puede implementar un punto central, así como lo sería una iglesia u otro edificio alto, y tiene varias interfaces de red por cable o inalámbrica que pueden ser atribuidas. Cuando se encuentra desplegado, B.A.T.M.A.N. puede transmitir datos de red en más de una dirección sin ningún retardo de retransmisión.

Ciertos fenómenos inusuales y circunstancias especiales podrían aparecer durante la determinación de la mejor ruta a través de la red. Estos han sido abordados y se contrarresta evitando la circulación por esa vía de enrutamiento (que puede impedir que los datos lleguen a su destino).

En esta versión, un nodo puede brindar informes a la red que proporciona acceso a Internet. Otros nodos utilizarán esa información para evaluar si existe una conexión a Internet cercana a ellos y cuál es el ancho de banda disponible. Se puede utilizar una puerta de enlace específica o permitir que B.A.T.M.A.N. determine qué puerta de entrada deberá utilizar en función de criterios tales como la velocidad de conexión.

Es en esta versión también que anuncia los dispositivos que no ejecutan B.A.T.M.A.N. por sí mismos. Por lo general, este método se utiliza para conectar redes de caseras a redes encadenadas. Por ejemplo, una instalación en el techo mediante una antena se conectará a la red inalámbrica a través de B.A.T.M.A.N. y el resto de la casa simplemente se dará a conocer, por lo tanto también estará accesible a la conexión.

Esta versión de B.A.T.M.A.N. ha demostrado que presentan altos niveles de estabilidad pero con los tiempos de convergencia ligeramente lentos en condiciones del mundo real, esto es confirmado por los análisis teóricos.

2.5.3. Robin (ROuting Batman INside)

Robin es un proyecto Open Source de Red MESH. La idea detrás de este proyecto es el poder conectar equipo inalámbrico (routers) de bajo costo (generalmente basado en un chip Atheros AP51), corriendo software libre.

Todo lo que se necesita es conectar un dispositivo a la toma de energía eléctrica y a un acceso a Internet (generalmente a través de un acceso xDSL), el mismo que hará las veces de Gateway.

2.5.3.1. Características:

• Construido sobre OpenWRT kamikaze

•Configuración automática (plug&play)

• Existe la posibilidad de escoger el Protocolo de Ruteo entre OLSR y BATMAN

• Nos la posibilidad de tener 2 SSID:

- ✓ Punto de acceso público con portal cautivo
- ✓ Punto de Acceso Privado con seguridad WPA-PSK

• Trabaja con los portales cautivos:

- ✓ NoDogSplash,
- ✓ CoovaAAA,
- ✓ worldspot,
- ✓ wifi-cpa
- ✓ con un Servidor RADIUS propio

• Soporta varios Dashboard entre ellos podemos mencionar:

- ✓ OrangeMesh
- ✓ CloudTrax
- ✓ Jo.ke.r

Al ser el proyecto Robin basado y concebido como software libre, puede redistribuirlo y / o modificarlo en los términos de la licencia GNUVersion 2.

2.5.3.2. Nodos ROBIN

Existen dos tipos de nodos en esta Red:

El nodo que ofrece conexión a Internet es llamado NODO GATEWAY.

Y un nodo sin ningún tipo de conexión a internet es un NODO REPETIDOR, este se conecta a través del protocolo MESH al GATEWAY

Estos nodos se pueden apreciar en la fig. 2.9

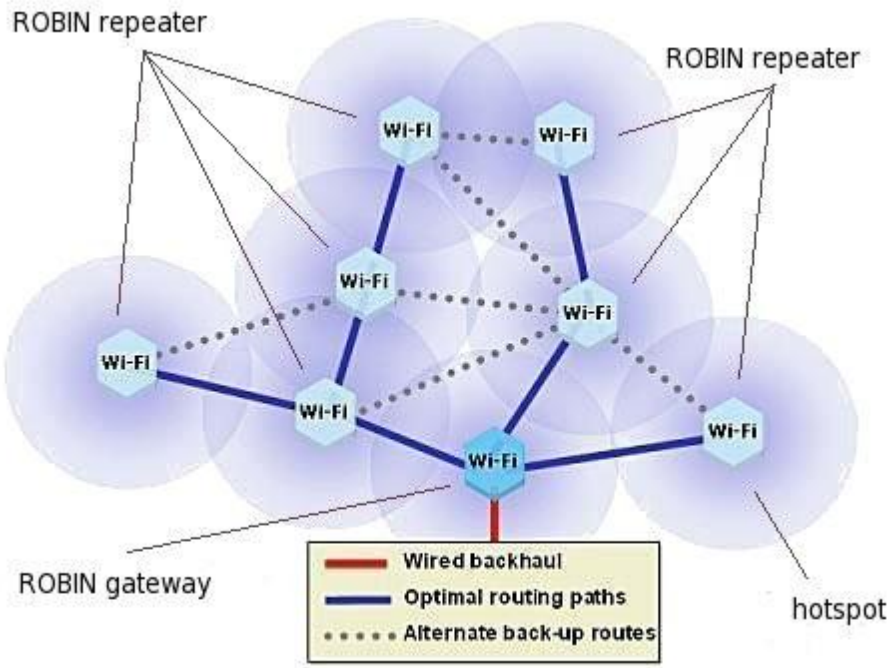


Figura 2.9.Topología de una red con protocolo ROBIN.

Cada nodo recibe paquetes de información (dependiendo del protocolo de ruteo) de los otros nodos activos de la red y se entera de la topología de red y el algoritmo de enrutamiento elegido (OLSR o Batman) se encargará de descubrir el mejor camino hacia un Gateway, para acceder al Internet.

Interfaces de un Nodo Robin

nodo	ath0	ath2	ath1	eth0
Gateway	Mesh y forward iface	WPAPSK AP2 iface Gateway por defecto para usuarios de la Wlan Privada	Open AP1 iface Gateway por defecto para usuarios de la Wlan Publica	Interface WAN
client	Mesh y forward iface	WPAPSK AP2 iface Gateway por defecto para usuarios de la Wlan Privada	Brlan (ath1 eth0 bridge) Gateway por defecto para usuarios de la WLan Publica y de usuarios de la red cableada	

Por lo general:

• El SSID Publico, AP publico o "AP abierto", (el punto de acceso virtual construido en ath1) es mencionado como AP1

• El SSID Privado, AP Privado, o "AP WPA-PSK ", (el VAP construido en ath2) es mencionado como AP2

Cabe indicar que el AP1 las interfaces eth0 y ath1 se encuentran punteadas si se trata de un nodo repetidor.

Rango de direcciones IP

Tanto AP1 como AP2 tiene activado un servidor DHCP que configurará las direcciones IP las estaciones conectadas a la red ya sean alámbrica o inalámbricamente.

Rango de la Red Mesh:

5.0.0.0/8, el mismo que se encuentra en el archivo de configuración /etc/config/mesh.

Rango de los APs: (2 subredes independientes por AP)

101.x.y.z/24 AP1

102.x.y.z/24 AP2

Todas las direcciones IP tiene relación con la dirección MAC del dispositivo

Si la MAC es aa:bb:cc:dd:ee:ff entonces la dirección de ath0 es 5.dd.ee.ff mientras las direcciones de ath1 y ath2 son: 101.ee.ff.1 y 102.ee.ff.1 (obviamente en formato decimal).

Por ejemplo las direcciones IP de un par de nodos serían:

•Nodo Cliente

dirección MAC: 00:18:0A:03:08:05

ath0: 5.3.8.5/8

ath1 y br0: 101.8.5.1/24

ath2: 102.8.5.128/24

Nodo Gateway

dirección MAC: 00:18:0 A:01:07:FE

ath0: 5.1.7.254

ath1: 101.7.254.1/24

ath2: 102.7.254.1/24

CAPITULO III

Diseño e Implementación de Red

1. Diseño

El diseño del proyecto piloto contiene lo siguiente:

- Elección de la ubicación
- Selección de la conexión a Internet
- Selección de la tecnología y los equipos a utilizar
- Ubicación
- Configuración
    - Configuración de firmware
- Herramientas de monitoreo
- Desarrollo del portal
- Cálculo de cobertura inalámbrica

1.1 Elección de la Ubicación del Proyecto Piloto

Al momento de determinar la ubicación del Proyecto Piloto se pensó en lugares que deberían cumplir con algunas especificaciones mínimas como:

1. Alto grado de concurrencia de personas
2. Acceso a la red eléctrica
3. Acceso a la Red Internet
4. Seguridad para personas y equipos
5. Infraestructura existente
6. Facilidades por parte de Autoridades

Los lugares que tentativamente se eligieron fueron:

1. Parque Recreacional Jipiro
2. Parque San Francisco
3. Mercado Centro Comercial
4. Parque Central
5. Campus del Área de la Energía, las Industrias y los Recursos No Renovables de la Universidad Nacional de Loja

A los mismos que se los sometió a una matriz de pesos de acuerdo a los criterios de selección enumerados anteriormente.

	1	2	3	4	5	6	TOTAL
1	X	-	X	-	-	-	2
2	X	-	-	-	-	-	1
3	X	X	X	X	-	-	4
4	X	-	-	-	-	-	1
5	X	X	X	X	X	x	6

Ponderación

X=1

-= 0

Tabla 3.1. Ponderación de Lugares

Como resultado de la ponderación se eligió al Campus del Área de la Energía, las Industrias y los Recursos No Renovables de la Universidad Nacional de Loja, como el sitio para la Implementación del Proyecto.

1.2 Selección de la conexión a Internet

El primer paso es disponer de conexión a Internet. Por lo general, el proveedor de acceso nos proporcionará un router con varias salidas LAN, alguna de las cuales podemos utilizar para conectar el nodo gateway. Las redes malladas funcionan como la red eléctrica de un país: cuantos más gateways (el equivalente a una central eléctrica), es decir, más conexiones a Internet tenga la red, mayor rendimiento para la conexión, más disponibilidad y menos latencia.

En primera instancia se pensó en conectarse a la red la Universidad Nacional de Loja, para así acceder a Internet, idea que luego fue desechada por los siguientes motivos:

- La administración Centralizada de la Red de la UNL, retrasaría los avances del Proyecto
- Se trata de una red muy grande (mas de 500 estaciones de trabajo) por lo tanto compleja.
- El firewall de esta red posee demasiadas medidas de seguridad que dificultan el trabajo con los diferentes puerto TCP y UDP
- La existencia de una DMZ (zona de desmilitarizada), con un proxy que autentifica por MAC , que dificultaría el libre acceso a la Red Mesh

Por las razones expuestas se opto por contar con un acceso ADSL proporcionado por la CNT.

1.3 Selección de Equipos y Tecnología a Utilizar

Equipos Mesh

Para la elección de los equipos MESH se tomó en cuenta los siguientes criterios:

1. Equipos que cumplan con el estándar 802.11b/g
2. Equipos que implementen o puedan implementarse protocolos de capa 3 (Router)
3. Equipos cuyo firmware este basado en LINUX y sean de tipo Open Source
4. De preferencia equipos basados en un chipset Atheros
5. De bajo/mediano costo

Tomando en cuenta estas características se escogió los equipos Accton MP3210A, también conocidos en España como La Fonera y es Estados Unidos como Open-Mesh.

Las características principales de estos equipos son:

- Dimensiones: 93,5 x 25,5 x 110 milímetros (sin contar la antena).
- Conector de antena: RP-SMA (SMA inverso).
- Antena exterior de 1,5 dBi.
- Autentificación WEP 64/128 bit, WPA, WPA2, WPAmixed.
- Cifrado TKIP, AES, mixed.
- Estándares WiFi IEEE 802.11b / 802.11g.
- 1 puerto Ethernet WAN (Internet) + 1 puerto Ethernet LAN.
- SSIDs: uno público y otro privado.
- CPU: 183.50 mhz
- RAM: 16 MB
- Flash: 8 MB
- Chipset Atheros AP51

Para una mejor descripción y conocimiento del equipo se adjunta el datasheet.

1.4 Ubicación de los equipos MESH

El factor fundamental a considerar para elegir los puntos de ubicación de los RouterMESH fue la cercanía con un punto de energía eléctrica, y luego el que al menos todos los edificios del Área de la Energía cuenten con un Router.

Por lo que la ubicación quedó como se puede apreciar en la el mapa realizado sobre Google Maps de la figura 3.1.

1.5 Configuración de Equipos

El primer paso para empezar a trabajar con los router es la instalación del Firmware R.O.B.I.N. en el dispositivo embebido.

Este proceso se lo realiza de la siguiente manera:

Primero, se necesita instalar un programa llamado WinpCap, el cual puede ser descargado desde:

http://www.winpcap.org/install/default.htm

Luego, procedemos a descargar y grabar el firmware desde:

http://dev.open-mesh.com/downloads/testing/firmware/open-mesh-flash.exe

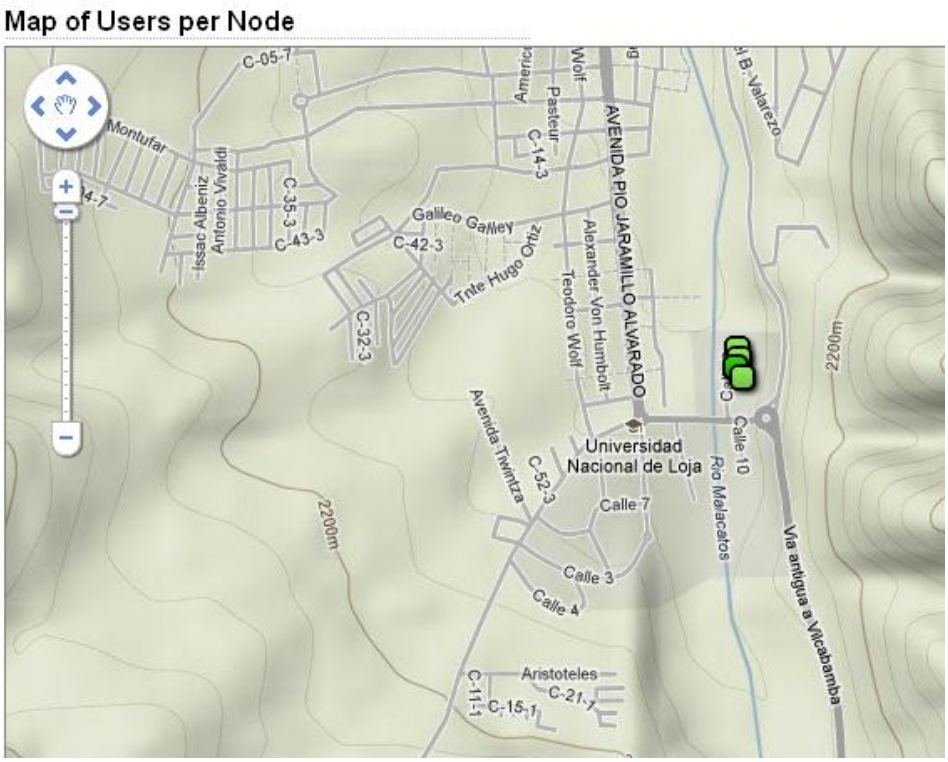


Fig. 3.1. Ubicación del proyecto

Esta es una aplicación que funciona desde la interfaz de comandos, de la siguiente manera:

C:\Users\Mike Asus\Downloads>open-mesh-flash
Usage:
open-mesh-flash [ethdevice] flashes embeddedkernel + rootfs: open-mesh firmware r2643
open-mesh-flash [ethdevice] rootfs.binkernel.lzma flashes yourrootfs and kernel
open-mesh-flash -v printsversioninformation

Esto nos indica que interfaces de red tenemos disponibles en nuestro PC, elegimos una que será la que esté conectada al router, generalmente es la Interfaz Ethernet:

1: \Device\NPF_{9BB97EBC-1BA2-4F39-93C3-A9841A4E863F}
    (Description: Sun)

2: \Device\NPF_{AAE405B9-0A93-4C4D-A3C7-E87BD8CB36E7}
    (Description: Microsoft)

3: \Device\NPF_{E789801D-D437-4BDA-9A7E-34BEC2058A0C}
    (Description: Atheros AtcL001 Gigabit Ethernet Controller)

4: \Device\NPF_{55143701-D657-4DEF-835A-14EEF2970416}
    (Description: MS Tunnel Interface Driver)

En este caso es la interface 3, digitamos el siguiente código y conectamos el router a la alimentación eléctrica.

C:\Users\Mike Asus\Downloads\open-mesh-flash 3

Peer MAC: 00:12:cf:c9:3c:ed
Peer IP : 192.168.0.1
Your MAC: 00:ba:be:ca:ff:ee
Your IP : 192.168.0.0
A flash size of 8 MB was detected.
rootfs(0x006a0000) + kernel(0x00100000) + nvram(0x00000000) sums up to 0x007a0000 bytes
Setting IP address...
Loading rootfs...
Sending rootfs, 4096 blocks...

Initializing partitions...
Rootfs partition size now 0x006b0000
Flashing rootfs...
Loading kernel...
Sending kernel, 1408 blocks...
Flashing kernel...
Setting boot_script_data...
Done. Restartingdevice...

1.6 Métodos y Herramientas de configuración del FirmWare

1.6.1 PUTTY

Hemos trabajado con el software Putty que nos permite acceder a través de Secure Shell SSH al router, bajo plataforma Windows.

La razón para acceder viaSSH es que el tamaño de las memorias FLASH y RAM no incluyen en el dispositivo una Interface Web.

El procedimiento para el acceso al firmware es:

Descargamos el paquete Putty desde:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

El software nos presenta una interfaz gráfica en donde entre otras cosas podemos escoger:

- Nombre del Host
- Puerto
- Tipo de conexión

Como se muestra en la figura 3.2

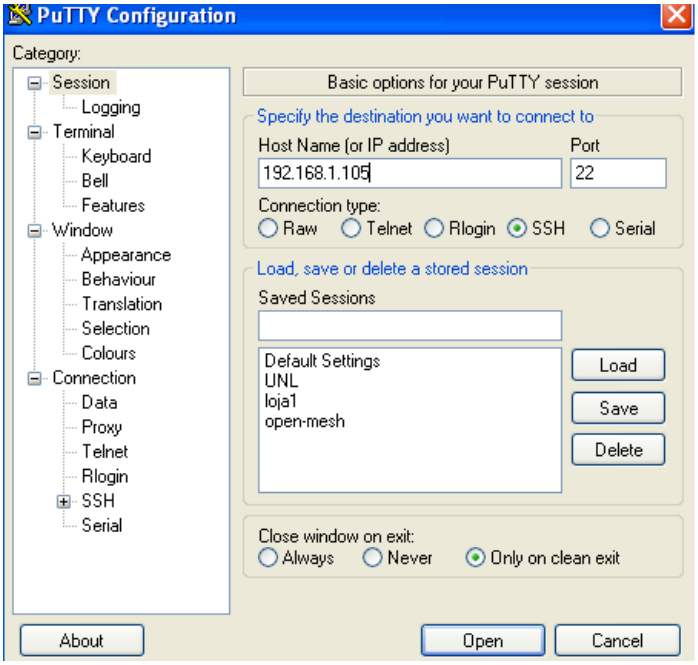


Fig. 3.2. Interfaz gráfica del Putty

Esto nos permite acceder a una interfaz de comandos en donde podemos configurar los parámetros del router tal como se indica en la figura 3.3

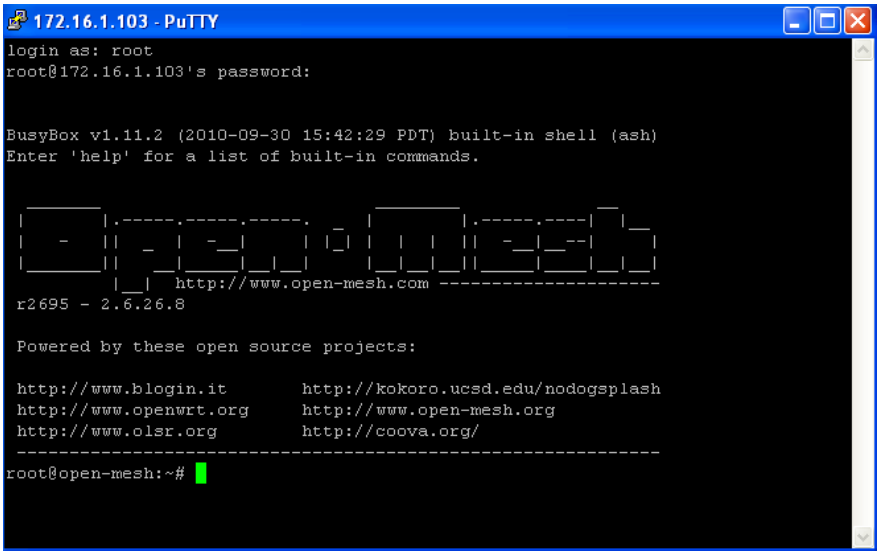


Fig. 3.3. Interfaz de comandos del Putty

A continuación se enlista los comandos más utilizados para la configuración.

Commands unique to open-mesh

logread Displays the log for the node

update	Forces an update of the node to the dashboard
upgrade	Forces the node to check for a software upgrade; might cause the node to lockup
olsrd-mon or olsrd-mon.sh	Displays the OLSR routing information
	Newer versions use olsrd-mon.sh to view the routing information
/sbin/channel	Forces the node to check for a channel change; use cmds below see when it will update on its own
askmara	Querys the built-in DNS server; format askmara Aopen-mesh.com. ; The A and are required
uci show node	Various info for the node; very useful command
free	Memory listing for the node: total, used, free
Wifi	Convert a ROBIN node into an access point (AP)
olsrd-mon.sh |less	olsrd info tables
olsrd-table.sh link	olsrd link table only

Stock Linux commands

crontab	Displaysthescheduledtasks
Date	Displays the current date and time for the node
ifconfig	Displays all of the network interfaces and there info
psaux	Displays the current running processes; static
top	Displays the current running processes; self updating (issues with this cmd w/ kernel 2.6.21)
uname -r	Displays the kernel version for the node
arp -av	Displays all of the current arp entries w/ names, if known
Vi	Built in text editor; look up cmds before using
route -n	IP routing table for fault finding network connections
olsrd-table.sh link	olsrd link quality table
cat/proc/net/madwifi/ath1 /associated_sta	The quality/SNR of the last frame received from a station is in the output

	of associated_sta in madwifi's tree under /proc. They label it rssi which ismisleading.
cat /proc/net/madwifi/ath0/ rate_info	rate_info gives you some clue to the quality of the return path.

Existe otra forma de configurar los router y es mediante el software WinSCP

1.6.2 WinSCP

WinSCP es una aplicación de Software libre. WinSCP es un cliente SFTP gráfico para Windows que emplea SSH. Su función principal es facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSHNewbie.

El código fuente de WinSCP y las descargas están hospedadas en SourceForge y se pueden bajar de:

http://winscp.net/eng/download.php

Al instalarlo nos presenta una interfaz gráfica, figura 3.4

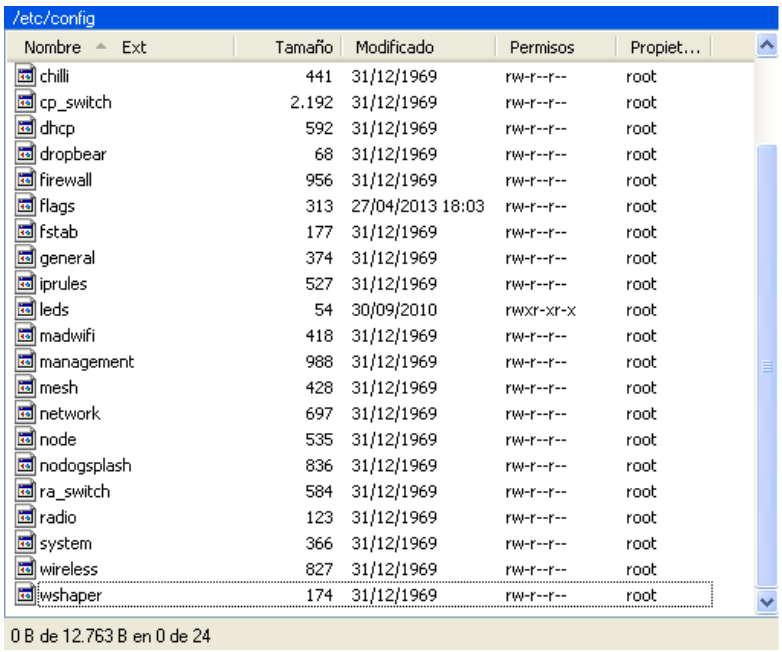


Fig. 3.4. Interfaz gráfica del WinSCP

De tal manera que podemos acceder a los archivos de configuración y editarlos directamente, los principales archivos son:

/tmp/dnsmasq.conf en este archivo podemos configurar el servidor DHCP

/etc/config/mesh/	en este archivo podemos configurar las características de la red mesh tal como: SSID, tipo de encriptación, claves de usuario
/etc/config/network	en este archivo podemos configurar las diferentes interfaces del router, sus direcciones ip y las máscaras de red
/etc/config/management	en este archivo podemos configurarlas opciones de administración de la red

1.7 Herramienta de Monitoreo (DashBoard)

La herramienta denominada Dashboard proporciona la facilidad de conocer el estado de la Red Mesh de forma remota.

Existen varias herramientas de este tipo en la actualidad, pero para su escogitamiento necesitábamos que cumpliera con las siguientes características

- Compatible con el Protocolo R.O.B.I.N.
- Que sea Open Source.
- Que cuente con una interfaz Web que nos permita acceder de forma remota a la red.
- Que permita cargar un portal de acceso HTML

Razón por la cual se escogió como Dashboard a la herramienta CloudTrax, la misma que tiene las siguientes características:

- Provee libre administración, alertas y mapeo para redes Mesh Basadas en R.O.B.I.N.
- Permite la configuración del SSID, portal cautivo Splash, paswords, y administración de ancho de banda
- Reportes diarios y alertas a través de e-mail.
- Diagrama de red y Nodos con sus respectivas conexiones durante las 24 horas.
- Estadísticas de los nodos
- Detalle del sitio a través de googlemaps

Esto lo logra a través de una interface web bastante intuitiva que presentamos a continuación:

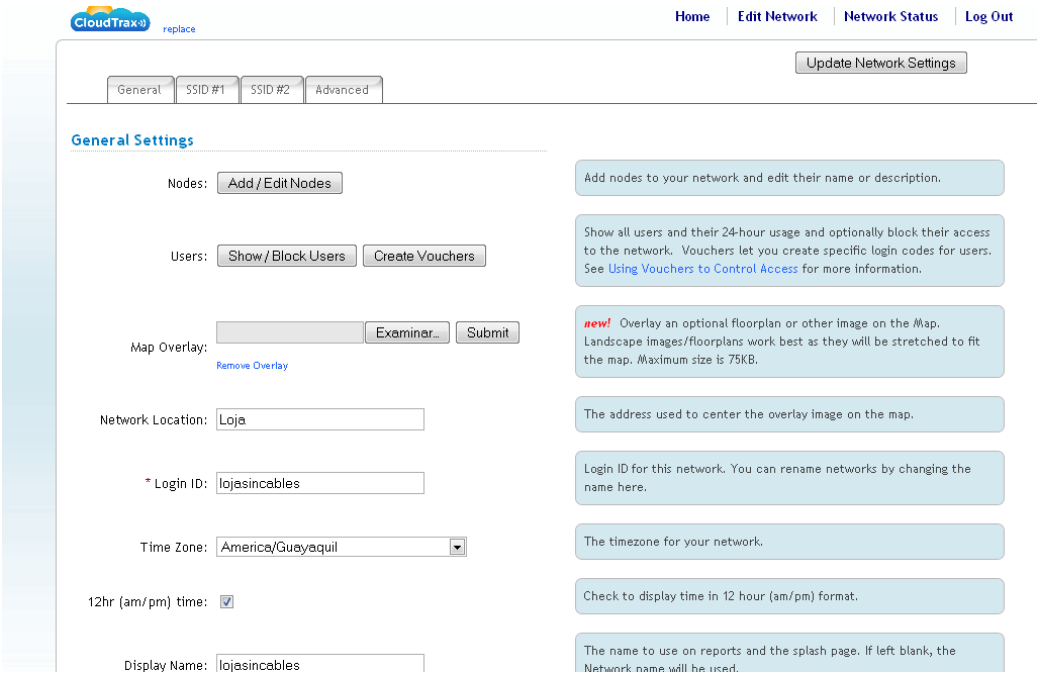


Fig. 3.5. DashBoard: Configuración General

En donde podemos observar:

- Configuración General (figura 3.5)
- Configuración del SSID 1 (figura 3.6)
- Configuración del SSID 2 (figura 3.7)
- Opciones Avanzadas (figura 3.8)

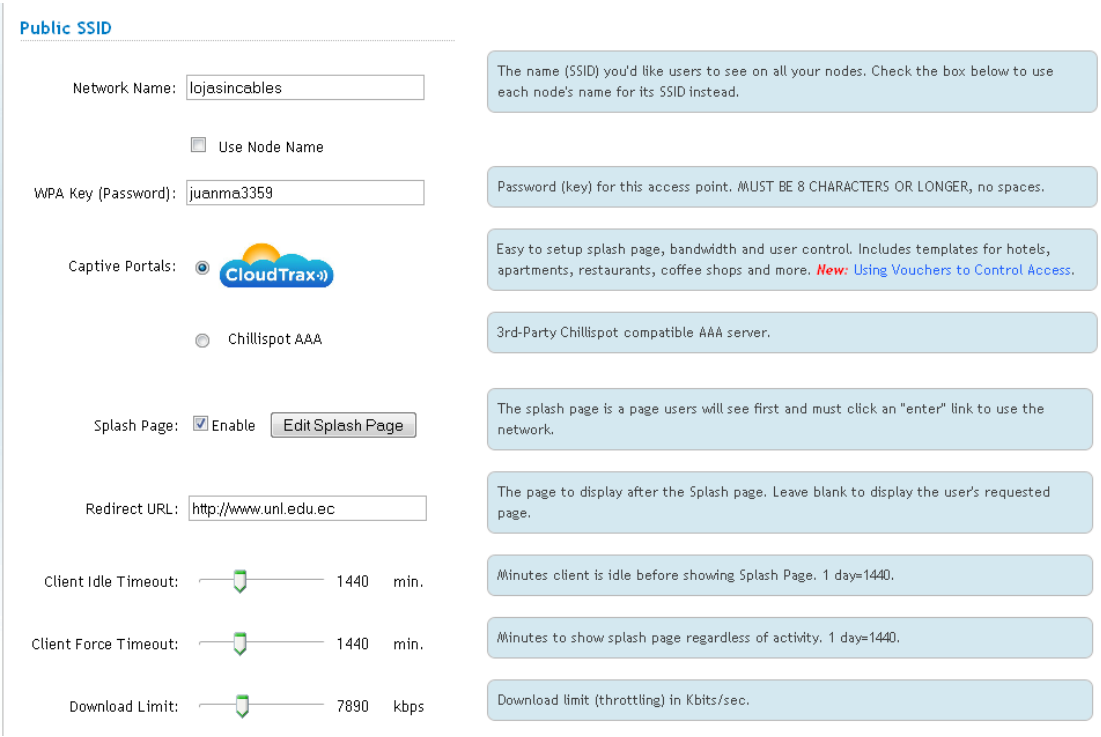


Fig. 3.6. DashBoard: Configuración SSID 1

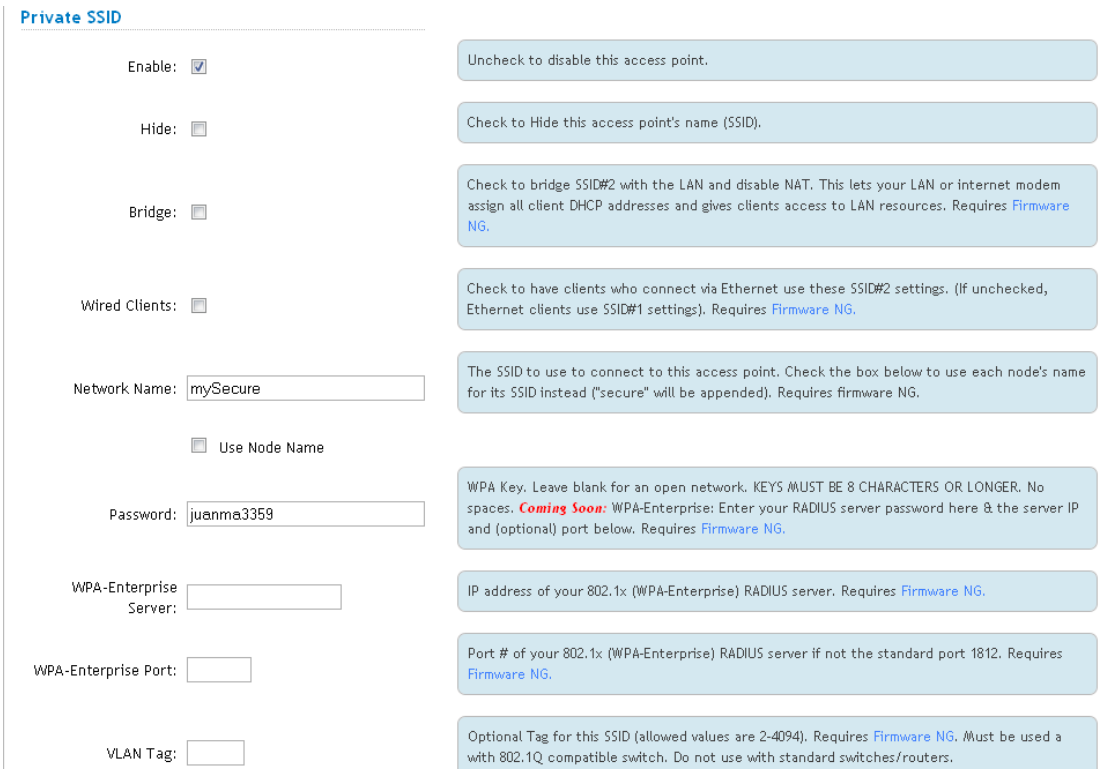


Fig. 3.7. DashBoard: Configuración SSID 2

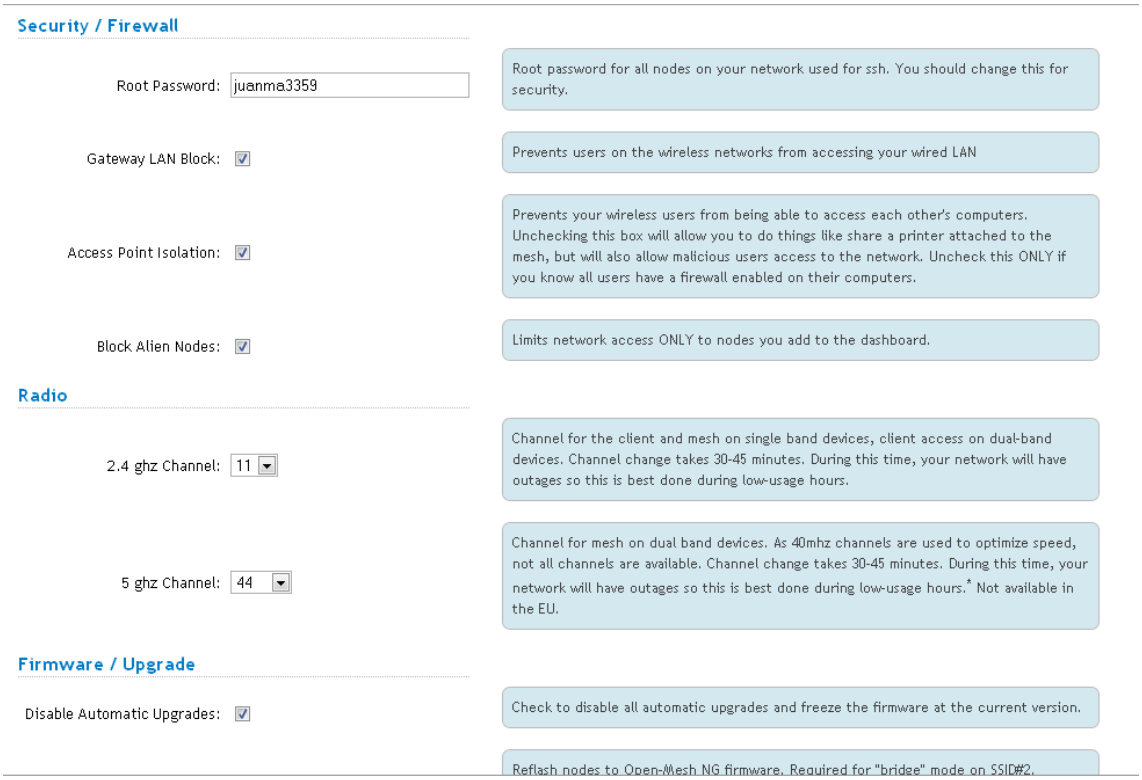


Fig. 3.8. DashBoard: Configuración Avanzada

Además esta herramienta, nos permite visualizar el estado de la red a través de las siguientes pantallas:

Status	name notes	mac ip	channel 2.4g/5g	24 hr users	24-hr usage MB down/up	up time	version	Load memfree	Last Checkin	gateway	hops	Ping Latency	Mes Last/
	NODO 3 Bloque de nivel tecnico	00:12:CF:8E:61:50 5.142.97.80	n/a n/a	0	0.0 0.0	0d:2h:47m -91	r2695-26/nO 0.5.6-r8	0.15 15.2	01 Mins	NODO 2 5.142.97.232	1	2	
	NODO 2 Poste de luz - Frente a copias	00:12:CF:8E:61:E8 5.142.97.232	n/a n/a	0	0.0 0.0	0d:2h:38m -91	r2695-26/nO 0.5.6-r8	0.13 15.4	08 Mins	self/192.168.1.1 190.12.13.243	0	n/a	n/ n/
	NODO 1 Antena	00:12:CF:8E:66:D8 5.142.102.216	n/a n/a	0	0.0 0.0	0d:2h:41m -91	r2695-26/nO 0.5.6-r8	0.13 15.0	03 Mins	NODO 2 5.142.97.232	1	3	
	NODO 4 Bloque 6	00:12:CF:8E:69:48 5.142.105.72	n/a n/a	0	0.0 0.0	0d:2h:48m -91	r2695-26/nO 0.5.6-r8	0.13 15.2	01 Mins	NODO 2 5.142.97.232	1	2	

Fig. 3.9. DashBoard: Estado de la Red MESH

La figura 3.9. nos permite visualizar todos los nodos de la red, sus direcciones MAC e IP, el tiempo que han estado UP en la red, su tasa de transferencia down/up, etc

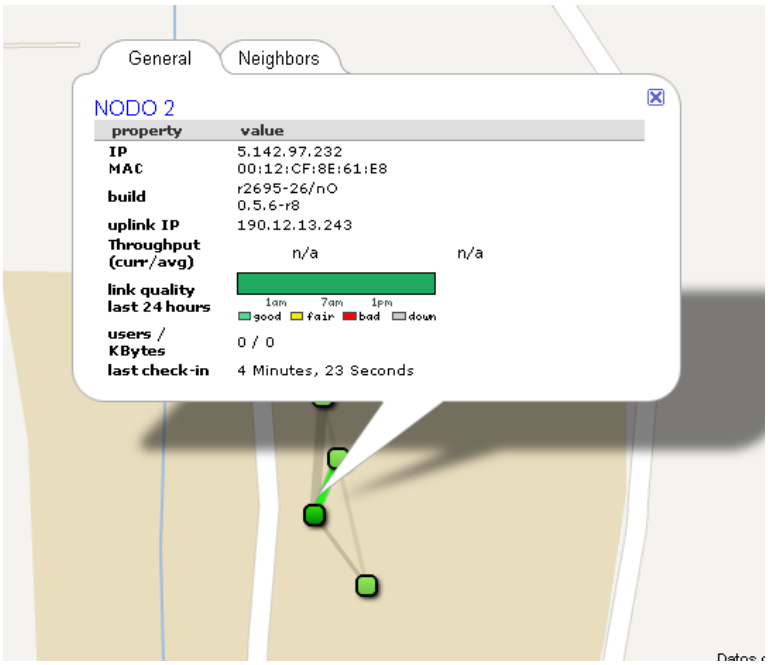


Fig. 3.10. DashBoard: Propiedades del nodo

La Figura 3.10. nos indica las características de cada nodo, su dirección MAC e IP, la versión del firmware, la calidad del link, etc.

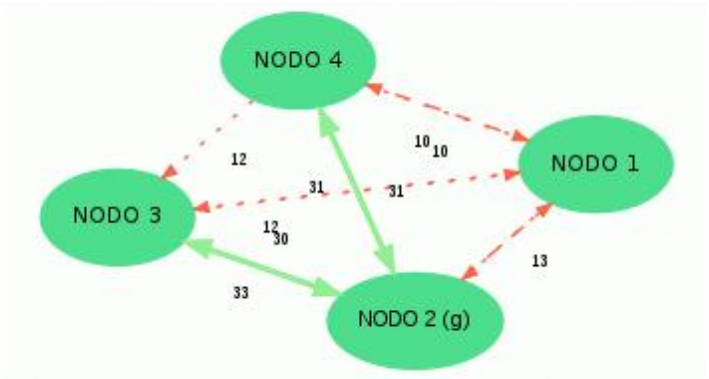


Fig. 3.11. DashBoard: Diagrama de Red

La Figura 3.11. nos indica cada nodo y sus enlaces con el resto de nodos, indicando la RSSI (Indicador de fuerza de señal de recepción) de cada enlace.

1.8 Desarrollo del Portal lojasincables

Ya que nuestro DashboardCloudTrax nos da la posibilidad de cargar un portal de acceso, se procedió a desarrollar el siguiente código HTML:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>Open-Mesh Wireless Routing</title>
<style type="text/css">

<!--
body {
background-color: #232;
margin:0px;
padding:0px;
text-align:center;
```

```
font-family: Georgia, "Times New Roman", Times, serif;
font-size:13px;
color:#252;
background:url(pattern_bg.gif);
line-height:20px;
}
#wrapper {
text-align:left;
margin:0 auto;
width:850px;
margin-top:18px;
border:2px solid #B4B744;
background:white;
}
a:hover {
color: #005080;
text-decoration: none;
}
a:link {
color: #00406A;
text-decoration: none;
}
.style1 {
font-size: 18px;
font-weight: bold;
}
.style2 {color: #999999}
-->
```

(Este segmento de código nos permite configurar el formato general del portal)

```
</style>
</head>
<body>

<div
id="wrapper"><imgsrc="/users/lojasincables/work/images/header.jpg"/><div
style="background: none repeat scroll 0% 0% rgb(204, 102,
0);"><imgsrc="/users/lojasincables/work/images/lady_laptop.jpg" style="margin-
right: 2px;"/><imgsrc="/users/lojasincables/work/images/fall.jpg" style="margin-
right: 2px;"/><imgsrc="/users/lojasincables/work/images/bike.jpg"
style="margin-right:
```

```
2px;"/><imgsrc="/users/lojasincables/work/images/family.jpg"/><br/>
<imgsrc="/users/lojasincables/work/images/divider.jpg"/></div>
```

(Este segmento de código nos permite visualizar las fotos, en otras palabras la imagen del portal)

```
<div style="background-image: url(bg.jpg); background-repeat: repeat-x;
background-color: rgb(255, 255, 255); padding-left: 190px; padding-right:
40px;">
<br/>
<span class="style1">Bienvenidos a lojasincables.org</span><br/>
<div style="float: right; width: 200px; margin-left: 15px; padding-left: 15px;
margin-top: 15px; border-left: 2px dotted rgb(153, 204, 0);">
```

(Este segmento de código nos permite visualizar el título del portal)

```
<p class="style9" align="left"><span
class="style24"></span>Yaereslibre!<br/></p>
<p class="style3" align="left"><span class="style18"><a
href="$authtarget"><imgsrc="/users/lojasincables/work/images/enter_green.jpg"
alt="Begin browsing" border="0" width="120" height="35"/></a></span></p>
<p class="style4" align="left"><br/></p>
</div>
```

(Este segmento de código nos permite visualizar una pequeña bienvenida, el slogan del portal "Ya eres libre" y presenta un botón para ir a la siguiente URL)

```
<p align="left">Este es un esfuerzo para la construcci&oacute;n de redes mesh,
teniendo como base la equidad y libertad.</p><p align="left">Este proyecto
basado en Software Libre, es una iniciativa para que las tecnologias de la
informaci&oacute;n sean una herramienta para el desarrollo de nuestros
pueblos.<br/></p>
Gracias!<br/>
Juan Ochoa Alde&aacute;n<br/>
<br/>
```

(Este segmento de código nos permite visualizar la presentación del portal, sus objetivos y su autor)

```
</div>
<imgsrc="/users/lojasincables/work/images/footer.jpg" width="850"
height="20"/></div>
<span class="style2">&copy; 2009 Open-Mesh</span><br/>
<br/>

</body>
</html>
```

El resultado de este código es el siguiente portal, figura 3.12.:

El código HTML nos permitirá visualizar el portal ***lojasincables***, en donde encontraremos información de la motivación del mismo, sus objetivos principales, su autor; pero lo más importante es que se presenta como una saludo a toda la comunidad que hace uso de esta red, permitiendo no solo el acceso a la siguiente URL que ***ucuenca.edu.ec*** sino también el poder llevar estadísticas de acceso al portal, otra parte importante es el hecho de dar la posibilidad al usuario de acceder o no a un portal, si el usuario está de acuerdo con las políticas del mismo.

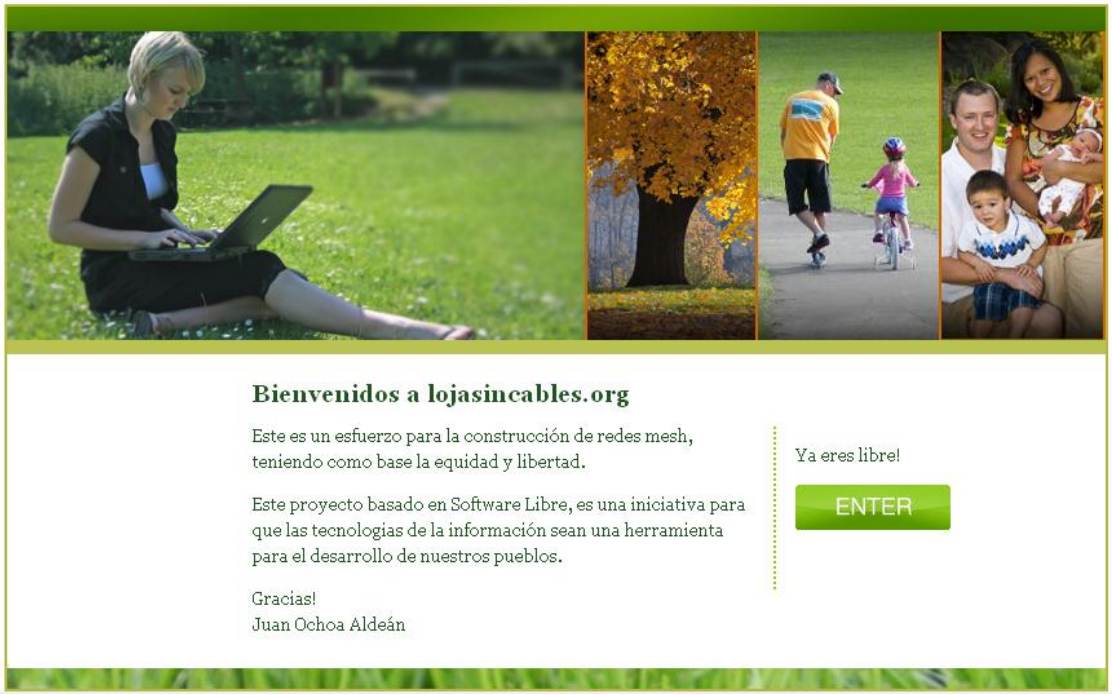


Fig. 3.12. Portal de acceso a la red MESH

1.9 Calculo de Cobertura Inalámbrica

Para el cálculo del diagrama de cobertura de la red hemos utilizado tres softwares, para comprender su aplicación hablaremos brevemente de ellos:

Netstumbler.- es un programa para Windows que permite detectar WLANs usando tarjetas wireless 802.11a, 802.11b y 802.11g. Tiene varios usos, como:

- Verificar que nuestra red está bien configurada.
- Estudiar la cobertura o señal que tenemos en diferentes puntos de nuestro domicilio de nuestra red.
- Detectar otras redes que pueden causar interferencias a la nuestra.
- Es muy útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.
- Sirve para detectar puntos de acceso no autorizados (RogueAP's).
- Por último, también nos sirve para detectar todos los APs que están a nuestro alrededor.

*EkahauHeatMapper.-*es una herramienta de software libre para determinar la cobertura de redes Wi-Fi (802.11).

HeatMapper también localiza los diferentes puntos de acceso y proporciona una visión en tiempo real para todos los puntos de acceso y sus configuraciones.

Sus principales potencialidades son:

- Muestra la cobertura Wi-Fi en un mapa
- Localiza todos los puntos de acceso
- Detéctala configuración de seguridad encuentra redes abiertas
- Soporta802.11n, así como a / b/g

Wolf wifi pro.- muestra las redes WiFi que están al alcance y el tipo de seguridad que tienen. También muestra el uso de los canales en una gráfica para ver los solapamientos, en realidad es muy similar a otros analizadores de WIFI pero la ventaja que tiene es que es para sistema operativo Android y puede ser instalado en un teléfono inteligente.

1.9.1 Método de trabajo

Como primer paso se procedió a ubicar los equipos de medición en el campus para ello se buscó lugares que presten las condiciones del caso, tales como protección de los fenómenos ambientales, energía eléctrica, etc...

Luego se procedió a instalar los programas antes mencionados de la siguiente manera:

- Netstumbler en una Laptop Toshiba NB100 con procesador Intel Atom, sistema operativo Windows XP
- HeatMapper en una Laptop Toshiba Satellite M645 con procesador Intel Core I3, sistema operativo Windows 7
- Wolf wifi pro en un teléfono inteligente Motorola Atrix 2 con procesador NVIDIATegra 2 AP20H Dual Core 1GHz, sistema operativo Android 2.3.6

Con la ayuda de la tabla 3. Podemos ubicar los nodos de acuerdo a su dirección MAC

NODO	NOMBRE	IP	MAC
1	NODO 1	5.142.102.216	00:12:CF:8E:66:D8
2	NODO 2	5.142.97.232	00:12:CF:8E:61:E8
3	NODO 3	5.142.97.80	00:12:CF:8E:61:50
4	NODO 4	5.142.105.72	00:12:CF:8E:69:48

Tabla 3.2. Información de Nodos

Y con ellos se procedió a tomar muestras en 10 lugares del campus los cuales se indican en la figura 3.13.

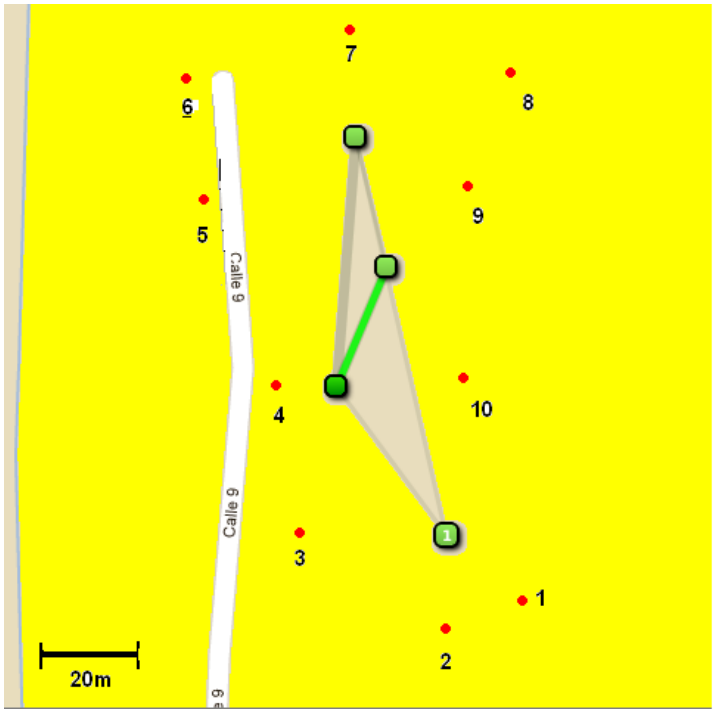


Fig. 3.13. Lugares de Medición

1.9.2 Datos tomados con Netstrumbler

Los datos tomados se pueden apreciar en una interfaz gráfica como la de la figura 3.14. y han sido ordenados en la tabla siguiente:

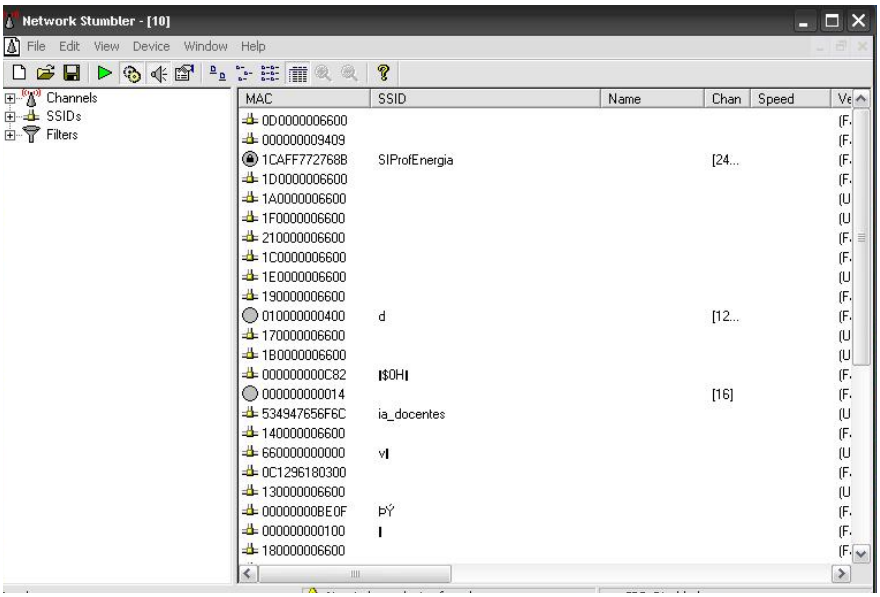


Fig. 3.14. Interface Gráfica del Netstumbler

A partir de los datos tomados en los 10 lugares señalados se tabulo la siguiente información:

Lugar	RSSI (dBm)	Ruido (dBm)	SNR(dB)	Calificación Señal
1	-65	-90	25	Muy Buena
2	-54	-90	36	Muy Buena
3	-72	-90	18	Baja
4	-50	-90	40	Excelente
5	-80	-90	10	Pobre
6	-77	-90	13	Baja
7	-64	-90	26	Muy Buena
8	-70	-90	20	Pobre
9	-65	-90	25	Muy Buena
10	-53	-90	37	Muy Buena

Tabla 3.3. Lugares de Medición de RSSI, Ruido y SNR

1.9.3 Datos tomados con EkahauHeatMapper

Los datos tomados se pueden apreciar en una interfaz gráfica como la de la figura 3.15.y nos permite trabajar sobre el mapa creado por Google Maps.

Fig. 3.15. Interface GráficaEkahauHeatMapper

Fig. 3.16. Aproximación de Cobertura Ekahau

La metodología consiste en caminar alrededor del área de cobertura y marcar la mayor cantidad de puntos posibles por donde se haya avanzado, el software nos presenta un aproximación de cobertura como la de la figura 3.16.

1.9.4 Datos tomados con Wolf Wifi

Este proceso fue utilizado como herramienta de medición para zonas de difícil acceso y para corroborar los datos entregados por el Netstrumbler.

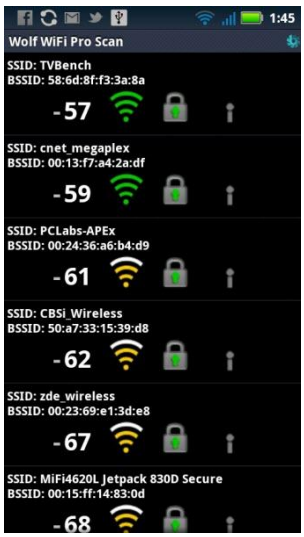


Fig. 3.17. Interface Gráfica Wolf Wifi

La interface gráfica del teléfono es la de la figura 3.17.

La información tomada en este procedimiento fueron incluidos en la tabla 3.

Los datos aportados por estos tres métodos han sido analizados y nos han dado como resultado el siguiente diagrama de cobertura de la red.

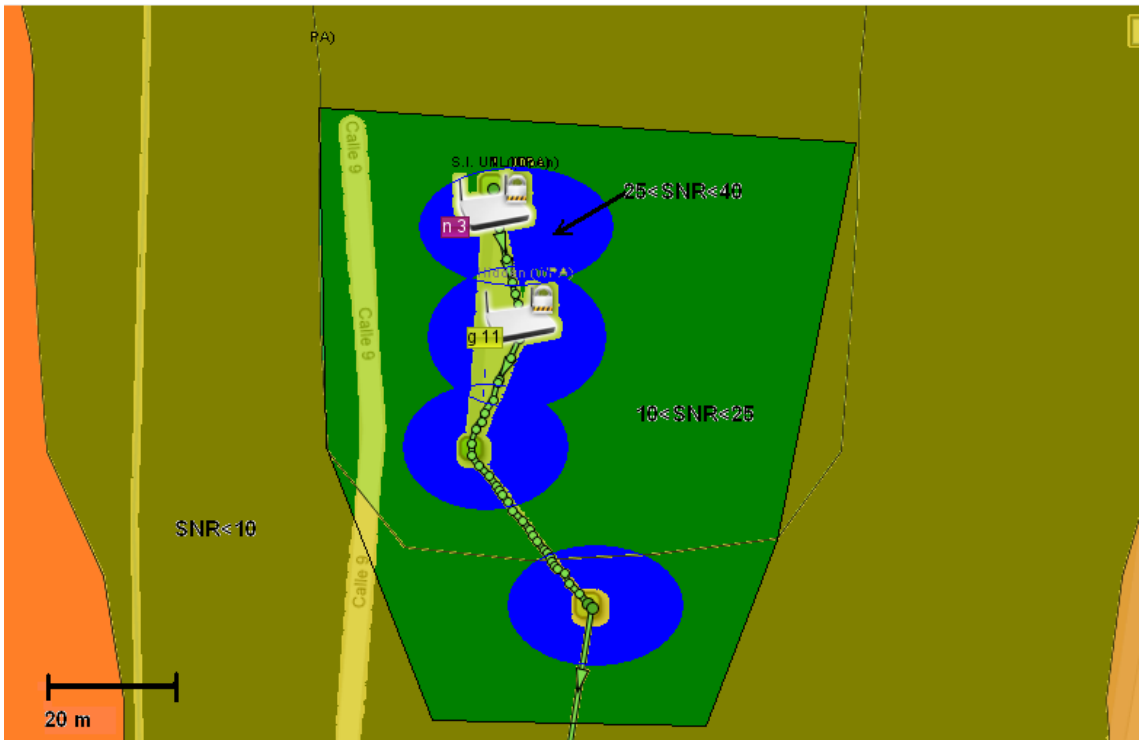


Fig. 3.18. Diagrama de Cobertura Inalámbrica de la Red Mesh

Luego de completar nuestro diagrama de cobertura y realizar mediciones en las de campo externas e internas (oficinas) en el campus podemos decir que la cobertura con una señal muy buena cubre a las principales dependencias del Área de la Energía, las Industrias y los Recursos Naturales No Renovables, tales como: Dirección del Área, Biblioteca, Secretaría Académica, Coordinaciones de Nivel y de Carrera, salas de Profesores entre otras.

CAPITULO IV

Pruebas Realizadas

El objetivo de este capítulo es someter a la red a pruebas que permitan medir algunos parámetros de la misma tales como: transporte de paquetes, manejo de protocolos, tasa de transmisión y retardo.

Las herramientas que nos permitirán llevar a cabo este objetivo son paquetes informáticos, tales como:

- Wireshark: transporte de paquetes y manejo de protocolos.
- Iperf: tasa de transmisión y retardo.

Estas pruebas determinarán las potencialidades y posibles fallas en la red, lo que permitirá evaluar la mitigación de errores y los mecanismos de gestión y planificación de expansiones en la red.

1. Instalación y manejo del Wireshark

Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación.

Permite examinar datos de una red en tiempo real o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

1.1 Aspectos importantes de Wireshark

- Mantenido bajo la licencia GPL.
- Trabaja muy duro tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).

- Basado en la librería pcap.
- Tiene una interfaz muy flexible.
- Gran capacidad de filtrado.
- Admite el formato estándar de archivos tcpdump.
- Reconstrucción de sesiones TCP
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.
- Puede traducir protocolos TCP IP
- Genera TSM y SUX momentáneamente

1.2 Instalación

Para instalar el Wireshark primero debemos instalar el software WinCAP en cual podemos bajar de: http://www.winpcap.org/install/default.htm

Una vez instalado podemos bajar el Wiresharkdesde:http://www.winpcap.org/install/default.htm

El Wireshark instalado nos presenta la siguiente interfaz gráfica:

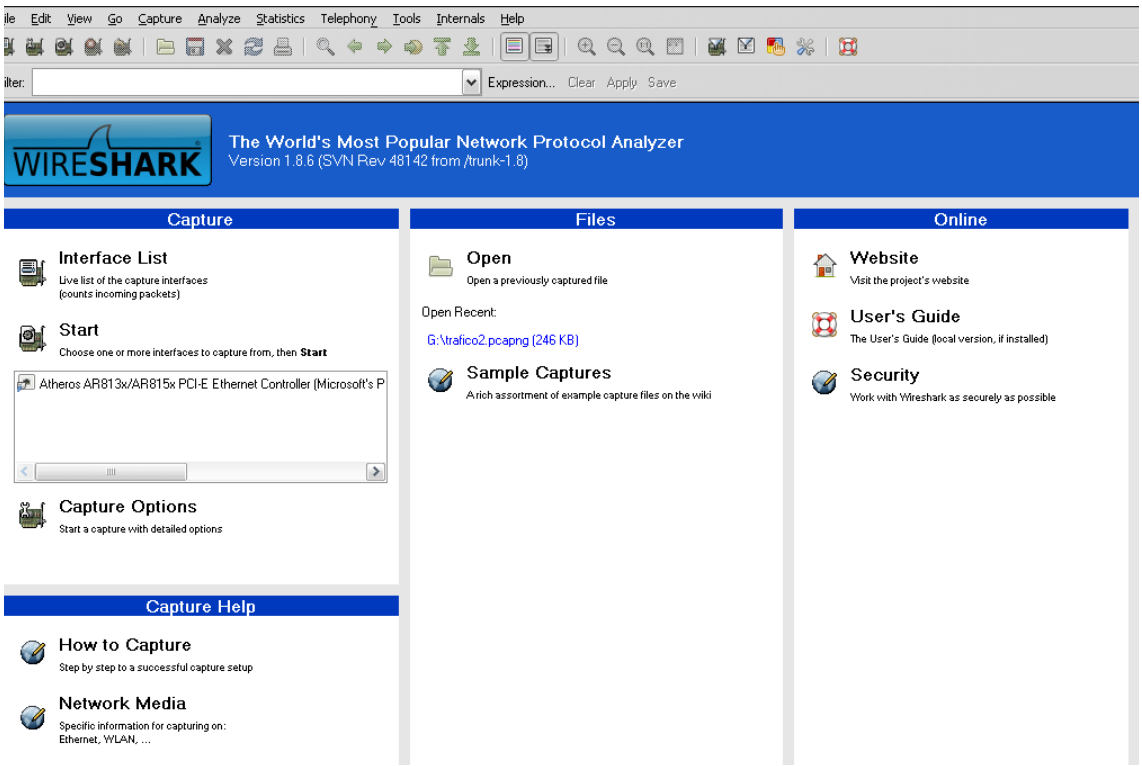


Fig. 4.1. Interfaz Gráfica del Wireshark

1.3 Prueba realizada

Se ha dispuesto 2 host ubicados en diferentes sectores de la cobertura de la red:

- El primero en el extremo sur del campus, este host generar trafico navegando en internet
- El segundo en el extremo norte, esta disposición para abarcar el mayor número de saltos, sobre este estará corriendo el wireshark, en modo promiscuo.

Se ha dispuesto que examine la red por alrededor de 60 minutos, pero para el análisis tomaremos algunas muestras aleatorias del trafico

Muestra 1:

667	908.915745	207.86.215.137	101.102.216.11	TCP	54 http > 49348 [ACK] Seq=3026 Ack=99 Win=5840 Len=0
668	908.915779	101.102.216.11	207.86.215.137	TCP	54 49348 > http [RST] Seq=99 Win=0 Len=0
779	931.868907	101.102.216.11	207.86.215.137	TCP	66 49349 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
780	931.872093	207.86.215.137	101.102.216.11	TCP	66 http > 49349 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1
781	931.872246	101.102.216.11	207.86.215.137	TCP	54 49349 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
782	931.872836	101.102.216.11	207.86.215.137	HTTP	151 GET /ncsi.txt HTTP/1.1
783	931.875847	207.86.215.137	101.102.216.11	TCP	54 http > 49349 [ACK] Seq=1 Ack=98 Win=5840 Len=0
784	931.886753	207.86.215.137	101.102.216.11	TCP	63 [TCP segment of a reassembled PDU]
785	931.894985	207.86.215.137	101.102.216.11	TCP	1514 [TCP segment of a reassembled PDU]
786	931.895100	101.102.216.11	207.86.215.137	TCP	54 49349 > http [ACK] Seq=98 Ack=1470 Win=17408 Len=0
787	931.899531	207.86.215.137	101.102.216.11	HTTP	1514 Continuation or non-HTTP traffic
788	931.899810	207.86.215.137	101.102.216.11	HTTP	125 Continuation or non-HTTP traffic
789	931.899868	101.102.216.11	207.86.215.137	TCP	54 49349 > http [ACK] Seq=98 Ack=3001 Win=17408 Len=0
790	931.900174	101.102.216.11	207.86.215.137	TCP	54 49349 > http [FIN, ACK] Seq=98 Ack=3001 Win=17408 Len=0
791	931.900201	207.86.215.137	101.102.216.11	HTTP	78 Continuation or non-HTTP traffic
792	931.900318	101.102.216.11	207.86.215.137	TCP	54 49349 > http [RST, ACK] Seq=99 Ack=3025 Win=0 Len=0

Fig. 4.2. Muestra de tráfico 1

Muestra 2:

697	913.013779	101.102.216.1	101.102.216.11	ICMP	90 Destination unreachable (Port unreachable)
698	913.417989	101.102.216.11	224.0.0.251	MDNS	313 Standard query response 0x0000 PTR, cache flush user-PC
699	913.645969	101.102.216.11	101.102.216.255	BROWSER	220 Request Announcement USER-PC
700	914.349970	101.102.216.11	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
701	915.146032	101.102.216.11	101.102.216.255	BROWSER	232 Browser Election Request
702	916.146056	101.102.216.11	101.102.216.255	BROWSER	232 Browser Election Request
705	916.225260	101.102.216.11	216.246.60.14	CLASSIC	62 Message: Binding Request
706	916.227684	101.102.216.1	101.102.216.11	ICMP	90 Destination unreachable (Port unreachable)
707	917.023587	fe80::8555:d8ff:24b	ff02::1:2	DHCPv6	149 Solicit XID: 0xdf9a27 CID: 0001000115fa9dc6b870f45673f6
708	917.146125	101.102.216.11	101.102.216.255	BROWSER	232 Browser Election Request
709	917.381576	101.102.216.11	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
710	918.005858	101.102.216.11	101.102.216.255	UDP	68 Source port: fmpro-internal Destination port: fmpro-int
711	918.146178	101.102.216.11	101.102.216.255	BROWSER	232 Browser Election Request
712	918.175077	101.102.216.11	224.0.0.251	MDNS	107 Standard query 0x0000 PTR _apple-mobdev._tcp.local, "QM
713	919.146302	101.102.216.11	101.102.216.255	NBNS	110 Registration NB WORKGROUP<1d>
714	919.438453	101.102.216.11	216.246.60.14	CLASSIC	62 Message: Binding Request

Fig. 4.3. Muestra de tráfico 2

Tanto en la figura 4.2. como 4.3. se puede observar el tráfico generándose del host 101.102.216.11, y utilizando los protocolos UDP,TCP, HTTL, ARP, RARP, DHCP

Del análisis podemos decir que los paquetes tanto UDP como TCP, transitan por la red sin ningún problema y con tiempos aceptables, tal como lo

demuestra la figura 4.4., en donde se realiza el análisis detallado de un paquete UDP

Es importante analizar qué pasa con el protocolo ICMP, cuando se envía uno de sus comandos más utilizados PING, tal como se muestra en la figura 4.5., el comando es recibido por nuestro router con su dirección MAC 00:12:CF:8e:66:d8 en un checksum correcto.

```
    Interface id: 0
    WTAP_ENCAP: 1
    Arrival Time: Apr 28, 2013 11:03:40.406181000 Hora est. del Pacifico de SA
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1367165020.406181000 seconds
    [Time delta from previous captured frame: 0.624282000 seconds]
    [Time delta from previous displayed frame: 0.624282000 seconds]
    [Time since reference or first frame: 918.005858000 seconds]
    Frame Number: 710
    Frame Length: 68 bytes (544 bits)
    Capture Length: 68 bytes (544 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  - Source: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c)
      Address: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
Internet Protocol Version 4, Src: 101.102.216.11 (101.102.216.11), Dst: 101.102.216.255 (101.102.216.255)
    Version: 4
    Header length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 54
    Identification: 0x10a3 (4259)
  + Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  + Header checksum: 0xae3c [correct]
    Source: 101.102.216.11 (101.102.216.11)
```

Fig. 4.4. Detalle de paquete UDP

```
Frame 715: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
  Interface id: 0
  WTAP_ENCAP: 1
  Arrival Time: Apr 28, 2013 11:03:41.843460000 Hora est. del Pacifico de SA
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1367165021.843460000 seconds
  [Time delta from previous captured frame: 0.004684000 seconds]
  [Time delta from previous displayed frame: 0.004684000 seconds]
  [Time since reference or first frame: 919.443137000 seconds]
  Frame Number: 715
  Frame Length: 90 bytes (720 bits)
  Capture Length: 90 bytes (720 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:icmp:ip:udp:classicstun]
  [Coloring Rule Name: ICMP errors]
  [Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmp
Ethernet II, Src: AcctonTe_8e:66:d8 (00:12:cf:8e:66:d8), Dst: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c)
- Destination: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c)
    Address: IntelCor_6f:8f:1c (8c:a9:82:6f:8f:1c)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
- Source: AcctonTe_8e:66:d8 (00:12:cf:8e:66:d8)
    Address: AcctonTe_8e:66:d8 (00:12:cf:8e:66:d8)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 101.102.216.1 (101.102.216.1), Dst: 101.102.216.11 (101.102.216.11)
  Version: 4
  Header length: 20 bytes
+ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 76
  Identification: 0xe0ba (57530)
+ Flags: 0x00
  Fragment offset: 0
  Time to live: 64
  Protocol: ICMP (1)
+ Header checksum: 0x1e5d [correct]
```

Fig. 4.5. Detalle de paquete ICMP

Una vez que se conoce el manejo del software y el formato en que presenta el tráfico y los paquetes tanto UDP como TCP, vamos a realizar pruebas con filtros lo que nos permitirá tener una idea clara de que está pasando con el tráfico que circula por nuestra red MESH.

1.3.1 Filtro paquetes TCP

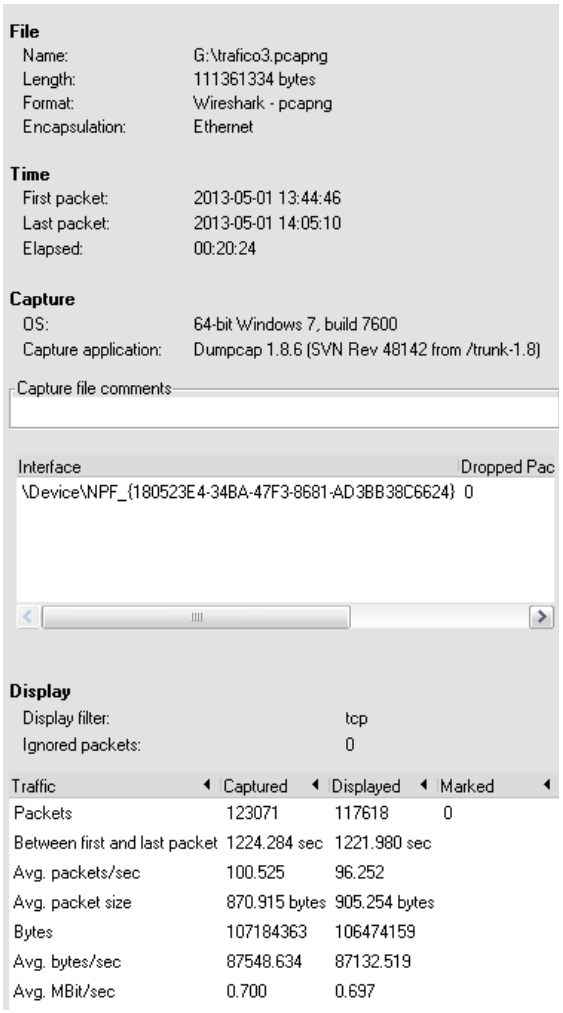


Fig. 4.6. Resumen análisis de trafico TCP

En la figura 4.6. podemos observar:

Tiempo de captura 20 minutos con 24 segundos

Filtro utilizado: tcp

Total de Paquetes: 117618

Promedio de paquetes por segundo: 96.252

Promedio del tamaño del paquete: 905.254 bytes

Bytes transmitidos: 106474159

Promedio de Bytes transmitidos por segundo: 87132.519

Además podemos obtener un informe especializado de los paquetes que tuvieron algún tipo de problema.

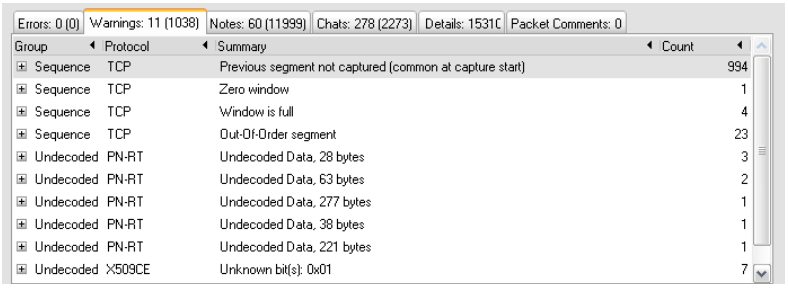


Fig. 4.7. ExpertInfo

De los resultados de la figura 4.7podemos concluir que de 123071 paquetes, 0 de ellos tuvieron errores, 11 presentan una precaución, es decir un 0.008%.

1.3.2 Filtro paquetes UDP

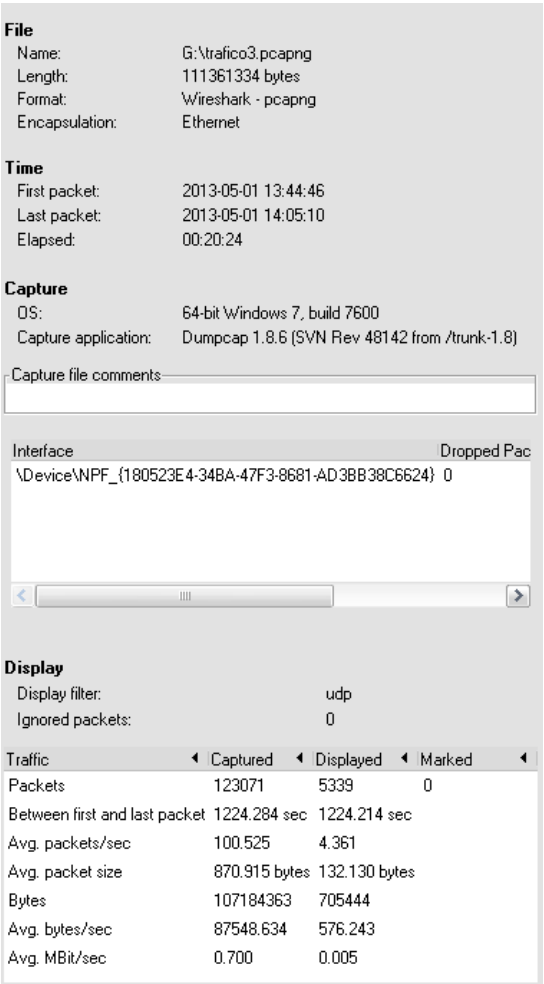


Fig. 4.8. Resumen análisis de trafico UDP

En la figura 4.8. podemos observar:

Tiempo de captura 16 minutos con 49 segundos

Filtro utilizado: udp

Total de Paquetes: 5339

Promedio de paquetes por segundo: 4.361

Promedio del tamaño del paquete: 132.13 Bytes

Bytes transmitidos: 705444

Promedio de Bytes transmitidos por segundo: 576.243

1.3.3 Gráfica Resumen de la prueba de tráfico

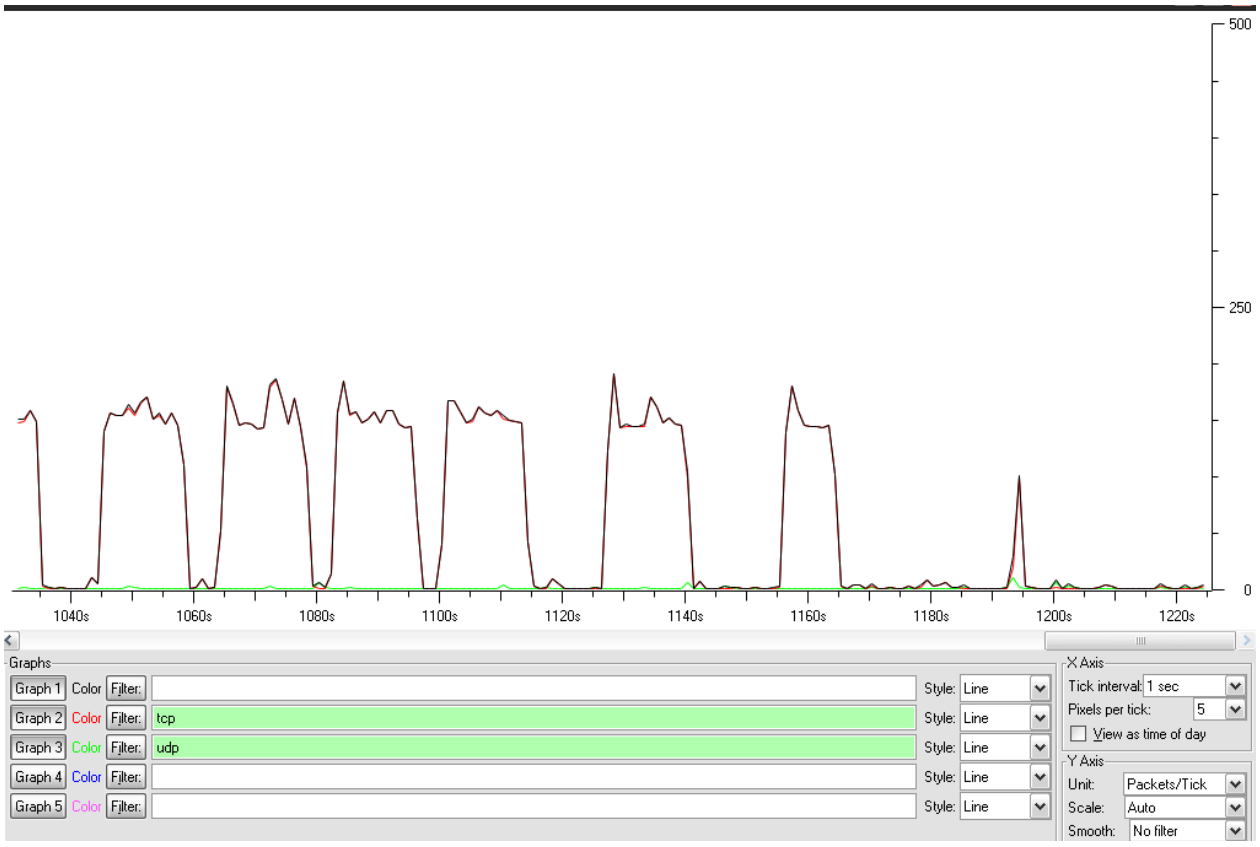


Fig. 4.9. Gráfica resumen análisis de tráfico

Figura 4.9.: en color negro podemos observar el tráfico total, con color rojo el trafico TCP y con color verde el trafico UDP

De la gráfica podemos decir que la mayoría del tráfico es TCP, con un 95.66% (117618 paquetes) frente al 4.34 % (5339 paquetes) de UDP, debido a que la prueba se realizó sobre un host navegando en internet (HTTP) que utiliza como protocolo de capa 4 a TCP.

Por lo que cualquier política se tome en cuanto al manejo del tráfico debe considerar que el principal protocolo a manejar va a ser TCP, ya que la finalidad de la red es ofrecer servicio de Internet.

2. Instalación y manejo del Jperf

2.1. Aspectos importantes de Jperf

Es una herramienta que nos permite medir el ancho de banda para el protocolo IP, nos proporciona información como la tasa de transferencia de datagramas en la red, el retardo (jitter) y la pérdida de paquetes. Todo ello enviando datagramas TCP o UDP según le especifiquemos y esperando la respuesta ACK.

Esta herramienta resulta útil para todo tipo de aplicaciones de red independientemente del protocolo de comunicaciones usado, permitiéndonos especificar el host, puerto, protocolo TCP o UDP; además puede correr en modo servidor o cliente.

```
Client/Server:
  -f, --format    [kmKM]   format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval  #        seconds between periodic bandwidth reports
  -l, --len       #[KM]    length of buffer to read or write (default 8 KB)
  -m, --print_mss          print TCP maximum segment size (MTU - TCP/IP
header)
  -p, --port      #        server port to listen on/connect to
  -u, --udp                use UDP rather than TCP
  -w, --window    #[KM]    TCP window size (socket buffer size)
  -B, --bind      <host>   bind to <host>, an interface or multicast address
  -C, --compatibility      for use with older versions does not sent extra msgs
  -M, --mss       #        set TCP maximum segment size (MTU - 40 bytes)
  -N, --nodelay            set TCP no delay, disabling Nagle's Algorithm
  -V, --IPv6Version        Set the domain to IPv6

Server specific:
  -s, --server             run in server mode
  -U, --single_udp         run in single threaded UDP mode
  -D, --daemon             run the server as a daemon

Client specific:
  -b, --bandwidth #[KM]    for UDP, bandwidth to send at in bits/sec
                           (default 1 Mbit/sec, implies -u)
  -c, --client    <host>   run in client mode, connecting to <host>
  -d, --dualtest           Do a bidirectional test simultaneously
```

```
-n, --num       #[KM]    number of bytes to transmit (instead of -t)
-r, --tradeoff           Do a bidirectional test individually
-t, --time      #        time in seconds to transmit for (default 10 secs)
-F, --fileinput<name>    input the data to be transmitted from a file
-I, --stdin              input the data to be transmitted from stdin
-L, --listenport #       port to recieve bidirectional tests back on
-P, --parallel  #        number of parallel client threads to run
-T, --ttl       #        time-to-live, for multicast (default 1)

Miscellaneous:
-h, --help               print this message and quit
-v, --version            print version information and quit
```

2.2. Instalación

Para instalar el JPERF primero debemos instalar la última versión de JAVA, luego de esto podemos bajar el paquete JPERF del sitio:

http://sourceforge.net/projects/jperf/

El JPERF instalado nos presenta la siguiente interfaz gráfica:

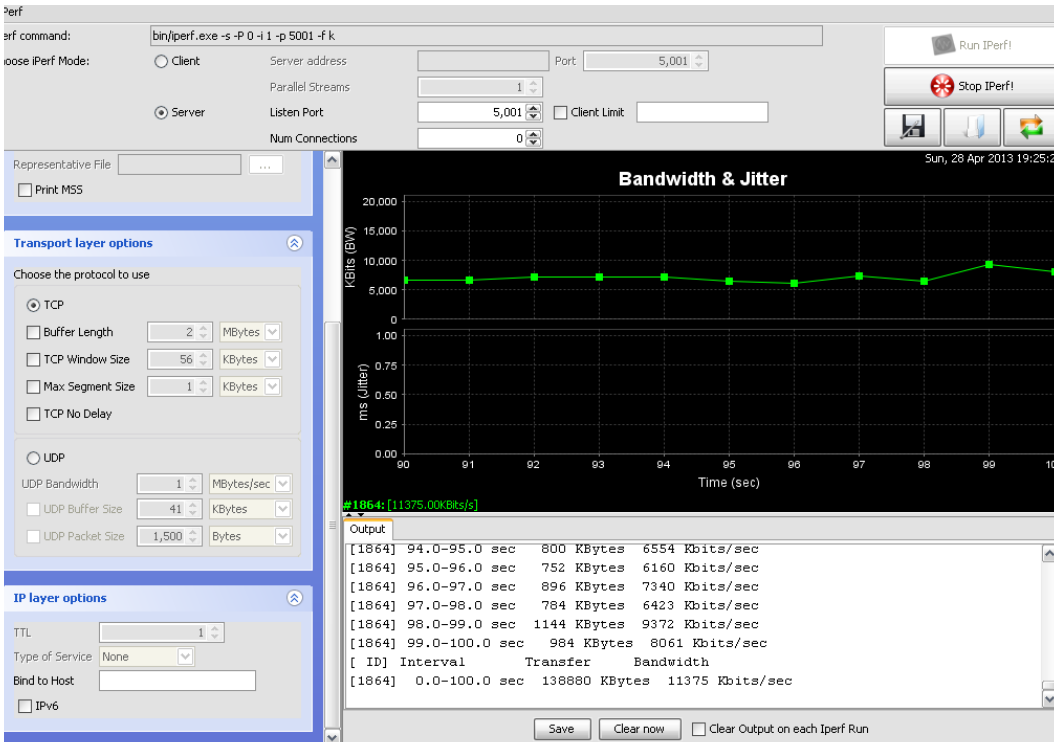


Fig. 4.10. Interfaz Gráfica del IPERF

2.3. Prueba realizada

En la prueba anterior el objetivo ha sido monitorear la calidad del tráfico, es decir los protocolos que viajan por la red y realizar un análisis partiendo de la

capa 4 del model0 OSI, es decir los protocolos UDP y TCP, en esta segunda prueba el objetivo es medir la cantidad de tráfico es decir la tasa de transmisión que se da entre dos puntos de la red, con dos host ubicados en los extremos de la misma, tal como en el caso anterior.

El primer host se lo configura como Server y se lo pone a escuchar el tráfico que se genera, el segundo host se lo configura como Cliente indicándole la dirección IP del servidor, además se asigna un tiempo de 3600 segundos para poder monitorear, pero para el análisis tomaremos algunas muestras aleatorias del tráfico, además se ha dividido el análisis en dos partes el tráfico con paquetes TCP y otro con UDP

Muestra 1: Trafico TCP

Fig. 4.11. Muestra de tráfico TCP

La grafica de la fig 4.11. nos muestra un tráfico para paquetes TCP constante alrededor de los 8 Mbps, tomando en consideración que los host se encuentran en los extremos de la red es una tasa de transmisión aceptable.

Muestra 2:Trafico UDP

Fig. 4.12. Muestra de tráfico UDP

La grafica de la fig 4.12. nos muestra un tráfico para paquetes UDP constante alrededor de los 8 Mbps, y un Jitter que no supera los 3 ms, por lo tanto la calidad de la red es Aceptable, incluso para redes que manejen tráfico sensible al retardo como Voz sobre IP (VoIP).

3. Mecanismos de gestión de Red.

Una red de cualquier tipo debe tener varios elementos que permitan su funcionamiento adecuado y son:

3.1. Gestión de red.

La gestión de red nos permite monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

Estas funciones se las realiza desde el dashboard, que una interfaz basada en la web donde el usuario puede administrar todos los nodos de la red, tanto los nodos como los gateways presentes en la misma, para nuestro caso hemos elegido ***cloudtrax*** al cual se puede acceder desde el siguiente link:

https://cloudtrax.com/dashboard.php

En donde se despliega una interfaz web con mecanismos de acceso como se puede apreciar en la figura 4.13.

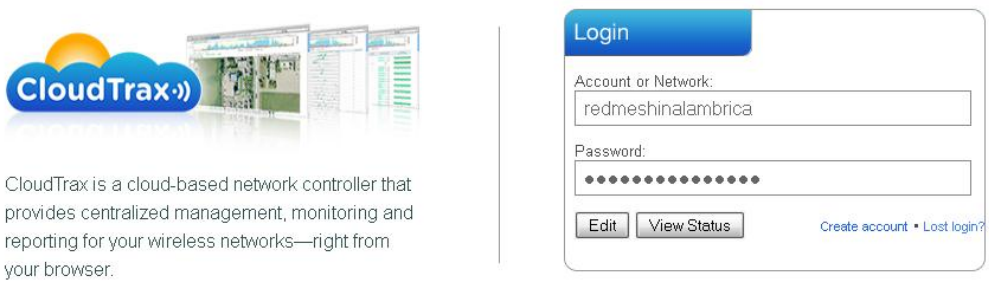


Fig. 4.13. Página de acceso a Cloudtrax

3.2. Gestión de seguridad y acceso a los recursos.

La seguridad de la red, al estar construida sobre IEEE 802.11 (WIFI), nos permite configurar cualquier de los protocolos de seguridad que posee el estándar, tales como:

- WEP
- WPA

- WPA2
- Autenticación por servidor RADIUS

Todos estos recursos son configurables también a través de ***cloudtrax***, como se puede observar en la figura 4.14.

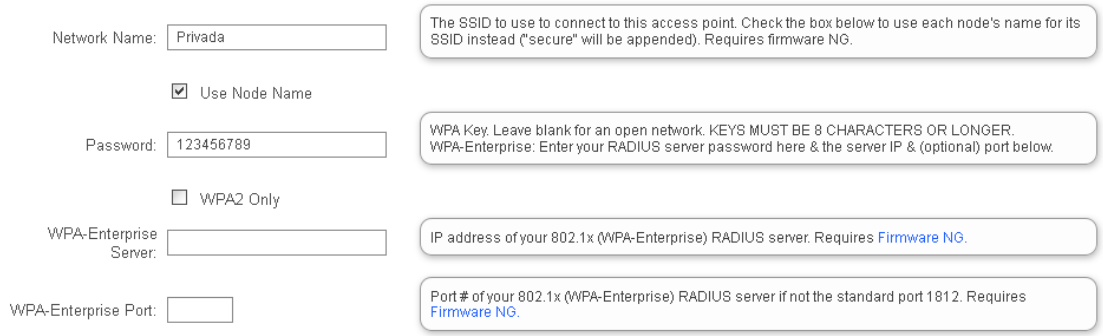


Fig. 4.14. Configuración de seguridades

Además el cloudtrax nos pemite acceder a información, tanto de lo nodos como de los usuarios tales como:

- Diagrama de red
- Direcciones IP
- Direcciones MAC
- Calidad del enlace
- Desempeño (throughput)
- Host conectados a la red
- Usuarios activos

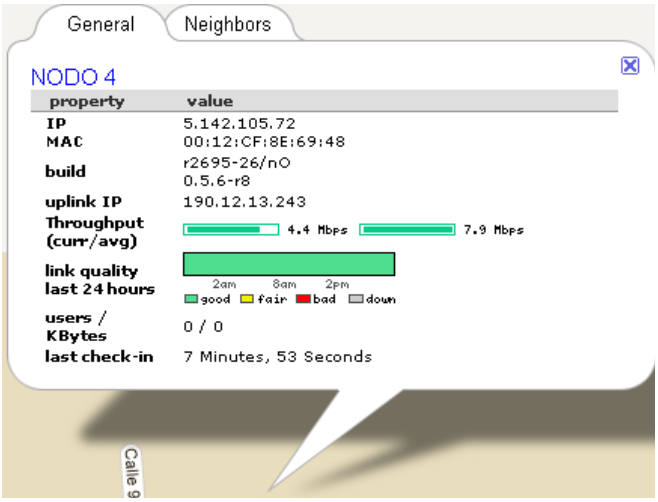


Fig. 4.15. Información de un nodo de la red.

Otra herramienta de seguridad que nos proporciona cloudtrax es el portal cautivo, este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

3.3. Redundancia

La redundancia está asegurada en el concepto de red mesh o mallada, ya que la misma es auto ruteable. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto.

El camino a seguir va depender del protocolo R.O.B.I.N que deberá cargar las tablas de ruteo en los nodos seleccionados como MPR y del intercambio de estas tablas entre nodos, mecanismos que se explican con detalle en el capítulo 2.

Podemos observar en la figura 4.16. como a través de cloudtrax podemos acceder a las rutas que se generan en nuestra red.

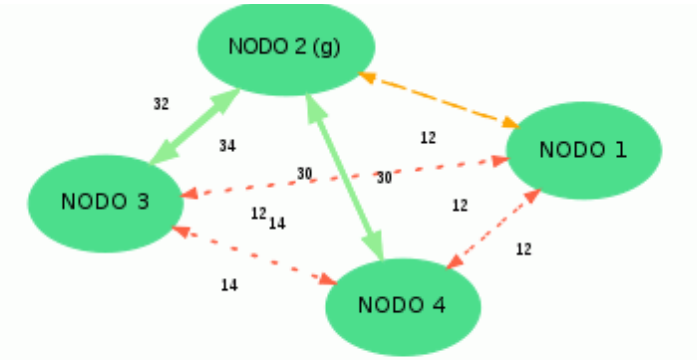


Fig. 4.16. Información de rutas de la red.

3.4. Plan de contingencias

Se ha diagramado un pequeño plan de contingencias en caso de ataques a nuestra red, basado siempre en el constante monitoreo a través de ***wireshark***.

Ataque: ARPSPOOF

Descripción

El ArpSpoofes comúnmente utilizado por atacantes para interponerse entre una o varias máquinas con el fin de interceptar, modificar o capturar paquetes. Se puede detectar cuando se está recibiendo gran cantidad de tráfico ARP. Si observamos más detalladamente el comportamiento del protocolo, nos daremos cuenta de que el servidor está siendo víctima de un ataque.

Herramientas como Ettercap, Cain y Abel o la suitDsniff permiten llevar a cabo este tipo de ataques sin necesidad de conocer en profundidad el funcionamiento de Ethernet o el protocolo ARP lo que incrementa su peligrosidad ya que un atacante no necesitaría tener conocimientos muy avanzados para capturar conversaciones de protocolos que viajen en claro, obtener contraseñas, ficheros, redirigir tráfico, etc.

Mitigación

Existen multitud de herramientas gratuitas destinadas a detectar este tipo de ataques tales como:

- Arpwatch
- Nast
- Snort
- PatriotNG
- ArpON, etc

Estas herramientas permiten generar alertas cuando se detecta un uso anormal del protocolo ARP.

Ataque: PORT FLOODING

Descripción

Consiste en enviar múltiples tramas falsificadas a través de un puerto con el objetivo de llenar la tabla de asignación del switch. Generalmente un switch dispone de una memoria interna denominada CAM (Content-Addressable Memory) donde asigna puertos a direcciones MAC. Cuando una trama llega a

un puerto, la CAM añade una entrada a la tabla especificando la MAC del equipo que envió la trama junto con el puerto en el que se encuentra. De esta forma, cuando el switch recibe una trama dirigida a ese equipo sabrá por qué puerto debe enviarla.

En caso de desconocer el destino de la trama, bien porque el equipo no ha llegado a generar tráfico o bien porque la entrada asociada a ese equipo ha expirado, el switch copiará la trama y la enviará por todos los puertos de la misma VLAN excepto por aquel por el que fue recibida. De esta forma, todos los equipos conectados al switch recibirán dicha trama y únicamente el equipo correspondiente, aquel cuya MAC coincida con la MAC destino de la trama, contestará; lo que permitirá al switch añadir una entrada a su tabla CAM con la nueva asociación MAC/puerto. Gracias a esto, el switch no necesitará inundar (flor) todos los puertos con futuros paquetes dirigidos a ese equipo.

Pero, ¿qué pasaría si se envían cientos de tramas falsificando la MAC origen del equipo y llenando la tabla CAM? En ese caso, su comportamiento depende del fabricante. Los switches de baja gama no contienen tablas CAM virtualizadas, es decir, que si la tabla dispone de un número n máximo de entradas para almacenar las asociaciones MAC/puerto, y un equipo consigue llenar dicha tabla con n entradas, la tabla se llenará y todas las VLANs se verán afectadas.

Con tablas CAM virtualizadas se mantendría un espacio de direcciones independiente para cada VLAN. De esta forma, sólo se verían afectados los equipos de la propia VLAN.

Yersinia o Macof permiten generar una inundación (*flooding*) de paquetes con MAC creadas aleatoriamente con el fin de saturar la tabla de asignaciones del *switch.*

Mitigación

Detectar este tipo de ataques usando un analizador de protocolos sería sencillo ya que, únicamente mirando el tráfico generado en ese tramo de red, veríamos gran cantidad de tramas con valores aleatorios.

Como se comentó anteriormente, este ataque daría lugar a una inundación (flooding) de paquetes en todos los puertos de esa VLAN (en el caso de usar tablas virtualizadas) una vez se llenara la tabla de asignaciones. Por lo tanto, también sería posible dejar escuchando a Wireshark en cualquier equipo de la misma y observar si se están recibiendo tramas no legítimas.

En cambio, con switches de gama media/alta es posible configurar ciertas características para mitigar este tipo de ataques. Algunos de los parámetros configurables son: el nivel de inundación (flooding) de paquetes permitido por VLAN y MAC (Unicast Flooding Protection), el número de MAC por puerto (portsecurity) y el tiempo de expiración de las MAC en la tabla CAM (aging time), entre otros.

Ataque: ANÁLISIS DE MALWARE

Descripción

El universo del malware es infinito y está constantemente en evolución. Sistemas antivirus implantados en servidores de correo o corporativos ofrecen unos resultados bastante aceptables pero siempre van un paso por detrás de las nuevas muestras y, por tanto, no son efectivos al 100% por lo que siempre se pueden dar casos de programas maliciosos que eluden estos sistemas y alcanzan el equipo del usuario final, consiguiendo ejecutarse.

Una vez que un equipo está infectado, resulta vital actuar con rapidez para minimizar el impacto que pueda tener en el propio sistema o en el resto de la organización por lo que es crucial identificar de qué espécimen se trata y eliminarlo.

Para comprender este ejemplo, supongamos que nos informan de que una máquina ha sido comprometida y que queremos identificar el vector de entrada y el tipo de malware involucrado. Para ello podemos echar mano de una captura de tráfico de red obtenida en una ventana de tiempo donde se haya producido el incidente. La abrimos con Wireshark para ver su contenido. Aislando las direcciones IP implicadas, y podemos identificar qué software se ha descargado aprovechando la utilidad de exportar objetos.

Suponemos que este archivo es malicioso por lo que habrá que tener cuidado de no abrirlo o ejecutarlo, pero ya tenemos una posible muestra del malware que podremos a analizar con nuestro antivirus o enviarla a que sea analizada online.

Mitigación

Este tipo de incidentes es difícil de mitigar. En general, se recomienda mantener los sistemas y aplicaciones lo más actualizadas posible y concienciar a los usuarios del peligro que supone la descarga de archivos desde fuentes no fiables o desconocidas, ya sea en documentos adjuntos al correo, como de enlaces web, aplicaciones P2P, etc.

Además de ataques la red puede sufrir de una serie de problemas adicionales, algunos de ellos se detallan a continuación con su respectivo plan de mitigación.

Optimización del Tráfico

La tasa de trasmisión se mide en bits por segundo (bps). Esto significa que dado suficiente tiempo, la cantidad de información transmisible en cualquier enlace se acerca al infinito. Desafortunadamente, para un período de tiempo finito, el ancho debanda provisto por una conexión de red cualquiera no es infinito. Siempre puede descargar (o cargar) tanto tráfico como quiera; sólo que debe esperar todo lo que sea necesario. Por supuesto que los usuarios humanos no son tan pacientes como las computadoras, y no están dispuestos a esperar una infinita cantidad de tiempo para que su información atraviese la red. Por esta razón, las tasa de transmisión deben ser gestionadas y priorizadas como cualquier otro recurso limitado.

Se puede mejorar significativamente el tiempo de respuesta y maximizar el rendimiento disponible mediante la eliminación del tráfico indeseado y redundante de nuestra red. A continuación se describen varias técnicas comunes para asegurarse de que nuestra red solamente está transportando el tráfico necesario para su correcto desempeño.

Mitigación:

Servidor Proxy

Un servidor web proxy es un servidor en la red local que mantiene copias delo que se ha leído recientemente, páginas web que son utilizadas a menudo, o partes de esas páginas. Cuando la siguiente persona busque esas páginas, las mismas se recuperan desde el servidor proxy local sin ir hasta Internet. Esto resulta, en la mayoría de los casos en un acceso al web más rápido, al mismo tiempo que se reduce significativamente la utilización del ancho de banda con Internet. Cuando se implementa un servidor proxy, el administrador debe saber que existen algunas páginas que no son almacenables, por ejemplo, páginas que son el resultado de programas del lado del servidor, u otros contenidos generados dinámicamente.

Además una política importante es evitar que los usuarios evadan el proxy, a través de las siguientes acciones:

• *No divulgar la dirección de la pasarela por omisión (default gateway) a través de DCHP*.- Esto puede funcionar por un tiempo, pero algunos usuarios que quieren eludir el proxy pueden encontrar o buscar la dirección de la pasarela

por omisión. Una vez que esto pasa, se tiende a difundir cómo se elude el proxy.

• *Utilizar políticas de grupo o de dominio.-* Esto es muy útil para configurar el servidor proxy adecuado para Internet Explorer en todas las computadoras del dominio, pero no es muy útil para evitar que el proxy sea eludido, porque se basa en el registro de un usuario en el dominio NT.

Un usuario con una computadora con Windows 95/98/ME puede cancelarse registro y luego eludir el proxy, y alguien que conoce la contraseña de un usuario local en su computadora con Windows NT/2000/XP puede registrarse localmente y hacer lo mismo.

• *Rogar y luchar con los usuarios.-* Ésta nunca es una situación óptima para un administrador de red. La única forma de asegurarse que los proxy no van a ser eludidos es mediante la utilización del diseño de red adecuado.

Almacenamiento intermedio (cache) y optimización de DNS

Los servidores DNS con sólo la función de cache no son autoridades de ningún dominio, solo almacenan los resultados de solicitudes pedidas por los clientes, tal como un servidor proxy que almacena páginas web populares por cierto tiempo. Las direcciones DNS son almacenadas hasta que su tiempo de vida (TTL por su sigla en inglés) expira. Esto va a reducir la cantidad de tráfico DNS en su conexión a Internet, porque el cache DNS puede ser capaz de satisfacer muchas de las preguntas localmente. Por supuesto que las computadoras de los clientes deben ser configuradas para utilizar el nombre del servidor solo de cache como su servidor DNS. Cuando todos los clientes utilicen ese servidor DNS como su servidor principal, repoblará rápidamente el cache de direcciones IP a nombres, por lo tanto los nombres solicitados previamente pueden ser resueltos rápidamente. Los servidores DNS que son autoridades para un dominio también actúan como cache de la conversión nombres-direcciones de hosts de ese dominio.

DNS dividido y un servidor duplicado

El objetivo de un DNS dividido (también conocido como horizonte dividido)es el de presentar una visión diferente de su dominio para el mundo interno el externo. Hay más de una forma de dividir DNS; pero por razones de seguridad se recomienda que tenga dos servidores de contenidos DNS separados; el interno y el externo (cada uno con bases de datos diferentes).

Dividir el DNS permite a los clientes de la red del campus resolver las direcciones IP para el dominio del campus a direcciones locales RFC1918,mientras que el resto de Internet resuelve los mismos nombres a

direcciónese diferentes. Esto se logra teniendo dos zonas en dos servidores DNS diferentes para el mismo dominio.

Una de las zonas es utilizada para los clientes internos de la red y la otra para los usuarios en internet.

3.5. Umbrales de operación normal e indicadores de congestionamiento.

Los umbrales de operación normales se podrán determinar midiendo el desempeño (throughput) de la red y la calidad de los enlaces, parámetros que nos proporciona cloudtrax, tal como se puede apreciar en la figura 4.17

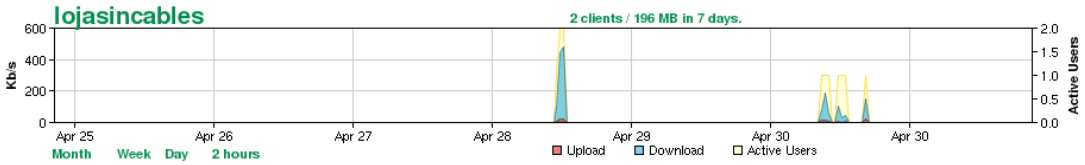


Fig. 4.17. Herramienta de monitoreo de Cloudtrax.

Tomando en cuenta que nuestra red opera sobre 802.11g se debe tener en cuenta los siguientes parámetros:

- La Tasa de transmisión necesaria para diversas aplicaciones, se puede observar en la figura 4.18.
- La relación señal a ruido SNR, medible mediante procesos indicados en el capítulo 3 debe estar dentro de los siguientes parámetros:
  - 40dBSNR= Excelente señal , siempre se conecta ; muy rápido.
  - 25dBa40dBSNR=Muy buena señal, siempre se conecta, muy rápido.
  - 15dB a25dBSNR= señal baja ,siempre conecta, por lo general rápido.
  - 10dB -15dBSNR=Muy baja señal, se conecta la mayoría de veces, lento.
  - 5dBa10dBSNR=No hay señal, no se conecta.

Aplicación	Ancho de Banda/ Usuario	Notas
Voz sobre IP (VoIP)	24 - 100+ Kbps	Como con el flujo de audio, VoIP dedica una cantidad constante de ancho de banda de cada usuario mientras dura la llamada. Pero con VoIP, el ancho de banda utilizado es aproximadamente igual en ambas direcciones. La latencia en una conexión VoIP molesta inmediatamente a los usuarios. Para VoIP una demora mayor a unas pocas decenas de milisegundos es inaceptable.
Flujo de video (streaming)	64 - 200+ Kbps	Como el flujo de audio, un poco de latencia intermitente es superada mediante la utilización de la memoria de almacenamiento temporal del cliente. El flujo de video requiere de alto rendimiento y baja latencia para trabajar correctamente.
Aplicaciones para compartir archivos Par-a-par (BitTorrent, KaZaA, Gnutella, eDonkey, etc.)	0 - infinitos Mbps	Si bien las aplicaciones par a par (peer-to-peer) toleran cualquier cantidad de latencia, tienden a utilizar todo el rendimiento disponible para transmitir datos a la mayor cantidad de clientes y lo más rápido como les sea posible. El uso de estas aplicaciones causa latencia y problemas de rendimiento para todos los otros usuarios de la red, a menos que se utilice un conformador de ancho de banda adecuado.

Aplicación	Ancho de Banda/ Usuario	Notas
Mensajería de texto / IM	< 1 Kbps	Como el tráfico es infrecuente y asincrónico, IM va a tolerar mucha latencia.
Correo electrónico	1 to 100 Kbps	Al igual que IM, el correo electrónico es asincrónico e intermitente, por lo tanto va a tolerar la latencia. Los archivos adjuntos grandes, los virus y el correo no deseado aumentan significativamente la utilización del ancho de banda. Los servicios de correo web (tales como Yahoo o Hotmail) deben ser considerados como navegadores web, no como correo electrónico.
Navegadores web	50 - 100+ Kbps	Los navegadores web sólo utilizan la red cuando se solicitan datos. La comunicación es asincrónica, por lo que se puede tolerar una buena cantidad de demora. Cuando los navegadores web, buscan datos voluminosos (imágenes pesadas, descargas largas, etc.) la utilización del ancho de banda aumenta significativamente.
Flujo de audio (streaming)	96 - 160 Kbps	Cada usuario de un servicio de flujo de audio va a utilizar una cantidad constante de una relativamente gran cantidad de ancho de banda, durante el tiempo que está activo. Puede tolerar algo de latencia pasajera mediante la utilización de mucha memoria de almacenamiento temporal en el cliente (buffer). Pero extensos períodos de espera van a hacer que el audio "salte" o que se den fallos en la sesión.

Fig. 4.18. Tasa de transmisión para diversas aplicaciones

Asignación de canales:

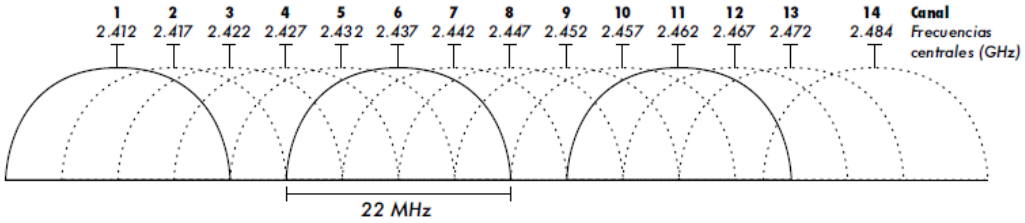


Fig.4.19. Canales y frecuencias centrales para 802.11

Sin dejar de ocupar NetStrumbler, IPERF, Ekahua, como instrumentos de medición para estos parámetros, como se detalla con profundidad en el capítulo 3 y al inicio de este capítulo.

CAPITULO V

1. CONCLUSIONES Y RECOMENDACIONES

1.1 CONCLUSIONES

En el presente trabajo de investigación se ha buscado el explicar los conceptos fundamentales de las redes MESH, tema sobre cual nada está definido, partiendo de que aun el estándar IEEE 802.11s para redes mesh no está completamente terminado, por lo que se trata de un tema abierto a muchas posibilidades, y si a esto le sumamos la cantidad de fabricante de equipo WIFI, el sinnúmero de protocolos para ruteo inalámbrico; el panorama se vuelve aún más complejo.

Por lo que la implementación de este piloto es un primer esfuerzo por conocer los protocolos MESH y sus aplicaciones, proyecto encaminado a ser uno de los peldaños para la integración del pueblo lojano y ecuatoriano a la Sociedad de la Información.

Luego de concluida la investigación se ha obtenido las siguiente conclusiones:

- Se ha implementado una red Mesh basada en el Protocolo R.O.B.I.N. en el Área de Energía, las Industrias y los Recursos Naturales No Renovables de la Universidad Nacional de Loja, la misma que será utilizada como herramienta de comunicación por la comunidad universitaria.
- Las redes Ad-Hoc no están limitadas a un grupo homogéneo de computadores, sino a cualquier dispositivo capaz de transmitir por un medio inalámbrico, es el caso de tabletas, teléfonos celulares inteligentes.
- Se testeado el protocolo R.O.B.I.N. que responde a las últimas tendencias en cuanto a redes inalámbricas, y además es una solución que trabaja con estándares abiertos, es decir software libre potenciando la investigación y desarrollo de nuevas soluciones tipo MESH.
- Mediante los paquetes IPERF y WIRESHARK hemos podido someter al protocolo R.O.B.I.N. a un buen número de pruebas, lo que nos ha

permitido comprobar su desempeño tanto con el protocolo UDP como TCP.

- El desempeño de un algoritmo de enrutamiento está dado por el uso de paquetes de control, lo cual tiene relación directa con el uso del ancho de banda disponible, el cual es limitado en las redes Ad-Hoc.
- Del análisis podemos decir que los paquetes tanto UDP como TCP, transitan por la red sin ningún problema y con tiempos aceptables, tal como lo demuestra la figura 4.4., en donde se realiza el análisis detallado de un paquete UDP
- La red Mesh implementada presenta una tasa de transmisión para paquetes TCP constante alrededor de los 8 Mbps, que es ACEPTABLE, pudiendo maneja trafico sensible a la perdida (Best-Effort) como por ejemplo: correo electrónico
- La red Mesh implementada presenta una tasa de transmisión para paquetes UDP constante alrededor de los 8 Mbps, y un Jitter que no supera los 3 ms, por lo tanto la calidad de la red es ACEPTABLE, incluso para redes que manejen tráfico sensible al retardo y que requieran un alto QoS como por ejemplo: Voz sobre IP (VoIP), audio y videoconferencia.
- La red Mesh implementada permite el trafico de todos los protocolos conocidos, en especial UDP y TCP, a nivel de capa 4 del Modelo de referencia OSI, lo que asegura que sobre la red puede correr cualquier tipo de aplicación

1.2. RECOMENDACIONES

Aunque, con este proyecto piloto hemos avanzado en la investigación acerca de las redes MESH, queda mucho camino por recorrer y es necesario seguir haciendo esfuerzos investigadores en este campo.

Motivo por el que cualquier recomendación está dirigida a las futuras ampliaciones de la red piloto y a otras implementaciones de redes Ad-doc la ciudad y el país.

- Primero es necesario aumentar el número de nodos para entrar al estudio de la sobrecarga en las tablas de enrutamiento y como estas afectan al desempeño de la red.
- Realizar pruebas en donde se incluya la movilidad de los dispositivos, lo que permitirá evaluar la red en dispositivos como tabletas, teléfonos inteligentes, que en un futuro no muy lejano manejarán la mayor cantidad de tráfico en este tipo de redes.

- Implementar redes Mesh en otro escenarios, como parques y centro urbanos, su análisis y estudio nos permitirán ir recabando información del desempeño de los protocolos en diferentes ambientes
- Otro reto será, el que una vez que se cuenta con la infraestructura para acceso a Internet en el AEIRNNR, el desarrollo de aplicaciones telemáticas, que potencien el uso de la red.
- Utilizar el proyecto piloto como una herramienta de pruebas de otros protocolos de enrutamiento MESH, ya que le hardware utilizado, basado en el chipset Atheros AP51 es muy versátil y posee muchos tipos de firmware inalámbrico compatibles.

BIBLIOGRAFIA

Subiela,Roberto,Simulación de protocolos de encaminamiento en redes móviles adhoc con SN-2, 30/04/2007.

Domingo,Mari,Diferenciación de servicios y mejora de la supervivencia en redes adhoc conectadas a redes fijas,2005.

Royer,Elizabeth,A Review of Current Routing Protocolos for AdHoc Mobile Wireless Networks,30/04/2007.

Mohapatra,Prasant,Ad Hoc Networks Technologies and Protocols, Springer Science,Boston 2005.

Redes inalámbricas para países en desarrollo. TerceraEdición 2012

Guerrero,Manel,Securing and Enhancing Routing Protocols for Mobile AdHoc Networks,09/05/2007.

DOUMENC,HELENE, ESTUDIO COMPARATIVO DE PROTOCOLOS DE ENCAMINAMIENTO EN REDES VANET, Universidad Politecnica de Madrid, Junio 2008

Ros, Francisco Javier, Evaluación de Propuestas de Interconexión a Internet para Redes Móviles Ad Hoc Hibridas, Universidad de Murcia, 2004

ANEXO 1

Data sheet Router M3201A

Accton
Making Partnership Work

MR3201A
1 Port Mini Router

The Accton mini router MR3201A is a wireless router with 1 WAN port with 2 SSID for private and public use purpose. It creates a wireless LAN environment that offers the security and WiFi phone functions at home and SOHO. There is a WAN port to connect your internet networking.

With the built-in security, manageability and reliability features, the MR3201A makes an ideal device for any Campus or SOHO users facing increasing mobile computing needs.

To protect communications and sensitive data on the wireless LAN, the MR3201A offers one of the most advanced and comprehensive set of authentication and encryption security capabilities on the market today.

The Accton MR3201A is a 802.11b/g wireless home router with 1 WAN port with 2 SSID for private and public use purpose. It creates a wireless LAN environment that offers the security and WIFI phone functions at home and SOHO.

Features and Benefits

Extra Security Protection

To protect your data and privacy, the MR3201A can encode all wireless transmissions with WEP or extra-strength WPA2 Personal encryption. Secure users' personal privacy at the enterprise level. Configuration is a snap with the Web browser-based configuration utility.

Multi-SSID Access Point

MR3201A is not a simple Access Point, it supports 2 SSID itself for enterprise to separate the user group, or it can helps the SOHO user to provide the private wireless access point for private users, and provide public wireless access point for others at the same time. The MR3201A saves space through integrating multi-function into a stylish device.

Cost-effective, secure, high-performance wireless connectivity

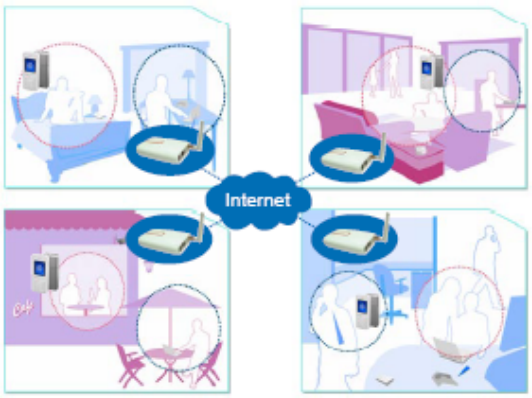
Designed for small offices home users and Campus. The MR3201A delivers the wireless networking with enterprise class performance and security in a single device. From remote employees in branch offices or simply in the home environment, this easy-to-deploy solution offers the flexibility to connect to the corporate private network, the Internet and more.

Support for multimedia applications

From simple to real-time demanding rich multimedia applications, the MR3201A delivers reliable performance. The Wi-Fi Multimedia 802.11e standard for Quality of Service and configurable dedicated SSID for Voice/Video enables you to take advantage of low cost call via Voice-over-IP.

For HOME
One SSID for private, one/sharing to public.

For SMB
One SSID for colleagues, one for customer.



For HOTSPOT
One SSID for private, one for public.

For COMPANY
One SSID for colleagues, one for customer.

Specifications

Network Interface
- 1 x RJ-45 10/100Mbps port
- 2 x 802.11b/g wireless interface

Gateway Features
- DHCP Server/Client
- Static IP
- NAT
- PPPoE

Wireless Features
- Interoperable with 802.11b/g compliant equipments
- Auto data rate switch with 1,2,5.5,6,9,11,12,18,24,36,48,54 for 11 b/g
- External Antenna
- Auto-Channel Selection
- System Throughput 22 Mbps

Security Features
- WEP 64/128/152-bit
- WPA/TKIP and PSK
- 802.11i(WPA2)
- 2 SSID

Management Features
- Web Based Management
- FTP/TFTP/HTTP download
- SNTP
- Event log
- System information
- Change Administrator Password
- System reboot

QoS Features
- 802.11e(WMM) basic (phase 2) *

Dimension
- Dimension (HxWxD): 90 x 60 x 146 mm

Power Supply
- External power adapter
- AC Input: 100-240V
- DC Output: 5V/2A

Environment Requirement
- The MR3201A complies with the following standards:
- Temperature: IEC 68-2-14
  - 0 to 40 degrees C (Standard Operating)
  - 0 to 70 degree C (Non-operation)
- Humidity: 5% to 95% (Non-condensing)
- Vibration: IEC 68-2-36, IEC 68-2-6
- Shock: IEC 68-2-29
- Drop: IEC 68-2-32

Emissions/Agency Approval/Safety
- US:FCC Part 15B & C
- Canada:ICES-003 & RSS-210
- Europe: EN 301 489-1 & -17, EN 300 328 EN 61000-3-2, EN 61000-3-3, EN 60950-1: 2001

Ordering Information
Model No: MR3201A

Contents:
MR3201A, mini router 11b/g Access Point
Power Adapter
User Manual (CD)
Quick Installation Guide (Hardcopy)
1 x RJ-45 Cable

* Specifications might change without notice

Accton Technology Corporation
International Headquarters :No. 1 Creation Rd. III,
Science-based Industrial Park, Hsinchu 300,
Taiwan, R.O.C.
Tel: 886-3-5770270
http://www.accton.com

DS_MR3201A_V.01
2006.12