UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA

TEMA: Estudio de una red de topología MESH para la Universidad del Azuay

TÍTULO PROFESIONAL AL CUAL SE ASPIRA:

INGENIERO ELECTRÓNICO

AUTOR

XAVIER ESTEBAN MORALES MEJÍA

DIRECTOR

LEOPOLDO CARLOS VÁZQUEZ RODRÍGUEZ

CUENCA - ECUADOR

2014

DEDICATORIA.

Esta tesis dedico a mi Padre y mi Madre; El Arq. Alberto Morales, La Maestra de Belleza Marcia Mejía que me ayudaron económicamente para que pueda alcanzar esta profesión, también que han estado juntos a mí apoyándome en todo momento. A todos que me dieron el apoyo para que no me rinda y siga luchando por mis ideales, sueños, ilusiones, proyectos, metas que tengo que alcanzar.

AGRADECIMIENTO

Agradezco a Dios, a mis Padres por el apoyo incondicional para poder cumplir este sueño y la colaboración que recibí de la Universidad del Azuay, especialmente por el personal de esta institución que me dio la posibilidad de desarrollar este tema.

ÍNDICE DE CONTENIDOS

CAPITULO 2. ANÁLISIS DE LA RED DE TOPOLOGÍA MESH

CAPITULO 3. ESTUDIO DE POSICIONAMIENTO DE LOS ACCESS POINT PARA DAR UNA MEJOR COBERTURA A LA UNIVERSIDAD DEL AZUAY

CAPITULO 4. CONFIGURACIÓN DEL ENRUTADOR MESH

CONCLUSIONES Y RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

Estudio de una Red de Topología MESH para la Universidad del Azuay

RESUMEN

Este trabajo de graduación fue realizado con el objeto de hacer un estudio para la implementación de una red de topología MESH como alternativa de solución a la red existente en la Facultad de Ciencia y Tecnología en la Universidad del Azuay a partir de un protocolo de enrutamiento llamado "DSDV" (Encaminamiento vector distancia), el cual es el responsable de realizar cálculos para la conectividad de los nodos entre: Computadores y Puntos de Acceso.

Los Procedimientos tomados en consideración fueron: Determinar los dispositivos de red adecuados para la topología, instalar el protocolo de enrutamiento, y cambiar las configuraciones de este mediante Linux.

Como resultado obtenido se logró mostrar una simulación del Protocolo de enrutamiento como propuesta para el diagnóstico de la red que puede ser utilizado futuramente para establecer enlaces que permitan la optimización de las topologías de red, sean de modo infraestructura, o modo Ad-hoc.

Palabras Clave: MESH, Inalámbrico, Ethernet, Ad-hoc, Punto de Acceso, D.S.D.V, Linux, Software, estándares de redes inalámbricas IEE802.11-WIFI, Red de Área Local-LAN, WLAN.

FRANCISCO VÁZQUEZ CALERO
DIRECTOR DE ESCUELA

LEOPOLDO VÁZQUEZ RODRIGUEZ
DIRECTOR DE TESIS

XAVIER ESTEBAN MORALES MEJIA
AUTOR

ABSTRACT

STUDY OF A MESH TOPOLOGY NETWORK FOR THE UNIVERSITY OF AZUAY

This graduation paper was carried out with the objective of conducting a study for the implementation of a MESH topology network as an alternative solution to the existing network in the Faculty of Science and Technology of the University of Azuay, parting from a routing called "DSDV" (Destination-Sequenced Distance Vector), which is responsible for calculating the connectivity of the nodes between computers and access points.

The following procedures were taken into consideration: determining the adequate network devices for the topology, installing the routing protocol and changing its configurations with Linux.

As a result, it was possible to display a simulation of the routing protocol as a proposal for the diagnosis of the network that can be used in future to establish links that will allow the optimization of the network topologies, either via infrastructure mode o ad-hoc mode.

KEYWORDS: MESH, wireless, Ethernet, ad-hoc, access point, DSDV, Linux, software, standards for IEE802.11-WIFI wireless networks, local area network, LAN, WLAN.

UNIVERSIDAD DEL AZUAY
ESCUELA Ingeniería Electrónica

(Signature and Seal)
FRANCISCO VAZQUEZ CALERO
SCHOOL DIRECTOR

(Signature)
LEOPOLDO VÁZQUEZ RODRÍGUEZ
THESIS DIRECTOR

(Signature)
XAVIER ESTEBAN MORALES MEJÍA
AUTHOR

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,
Melita Vega

Xavier Esteban Morales Mejía
Trabajo de Graduación
Director: Leopoldo Vásquez
Abril del 2014

INTRODUCCIÓN

La razón que me motivó hacer este tema, es porque surgió una necesidad grande por el estudio de una red de topología MESH. Las redes MESH ya fueron utilizadas para aplicaciones de tipo militar, y en los campus en universidades donde la señal de red inalámbrica de datos es inasequible.

Este trabajo está elaborado para hacer el estudio de una red de topología MESH para la Universidad del Azuay, en el Campus de la Facultad de Ciencia y Tecnología.

El objetivo es ilustrar una red de topología MESH compuesta de los siguientes nodos: un nodo servidor, y varios nodos clientes. La infraestructura de la red tiene la finalidad de ampliar la cobertura de la señal de radio, permitiendo una mejor movilidad de los clientes a mayores distancias.

El servidor para el protocolo de enrutamiento en redes de topología MESH (DSDV) seimplementa en una plataforma Gnu/Linux (En la versión del kernel 2.6.38+).

Los nodos de la red se encuentran distribuidos en modo ad hoc. El servidor de enrutamiento realiza un diagnóstico instantáneo de la red cada vez que un nuevo nodo quiere registrarse.

Cualquier dispositivo con capacidad de acceso inalámbrico, compatible con la tecnología MESH, puede adherirse a la red como un cliente, o como un terminal de distribución sea en topología “ad hoc” o en modo infraestructura.

Las configuraciones necesarias para estos dispositivosse graban en sus memorias RAM FLASH, con un programa de tipo OpenWrt.

CAPÍTULO 1

TEORÍA DE LAS REDES DE TOPOLOGÍA MESH.

1.1. Cronología de las redes MESH.

En Junio de 1971 se inician los proyectos para el desarrollo de las primeras redes inalámbricas de computadoras. ALOHAnet y PRNET implementan una red Ad-hoc sobre una red de datos básica. En la misma década, la firma DARPA maniobra en frecuencias UHF, y más tarde AMPRNet implementa el protocolo TCP/IP con su propio rango de direcciones IP reservado. (Sevilla Mesh, 2011).

En la década de los 80s, bajo el nombre de "Proyecto SURAN (Survivable radio Network), DARPA crea una red Ad-hoc con capacidad de movilidad de bajo coste.

Los clientes de red podían moverse, aparecer y desaparecer dentro de la red. Este tipo de red se denomina en la actualidad como MANET (Mobile Ad-hoc Network).

En la década de los 90s, la amplia difusión de la Internet y de los dispositivos portátiles (teléfonos celulares, PDA's, laptops, etc), fomentaron el desarrollo de las redes inalámbricas, cuando estas empezaron a ser una alternativa más eficiente a las redes cableadas,en aplicaciones civiles y comerciales.

En 1997 el ejército de EE.UU. comenzó el desarrolló del Tactical Internet (TI), que implementó en una red inalámbrica, paquetes de radio multi-salto,permitiendo la conformación de un campo de batalla militar totalmente digitalizado, en el que cada unidad tiene comunicación bidireccional de datos con todas las demás.

El IEEE (Institute of Electrical and Electronics Engineers) aprobó el estándar 802.11, que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando las normas de funcionamiento en una red local inalámbrica (WLAN, Wireless Local Area Network). Simultáneamente, se desarrollaron estándares como Bluetooth e HIPERLAN.

En 1999, se revisa el estándar 802.11, aumentando la velocidad de transferencia de las comunicaciones inalámbricas hasta los 11Mbps, y dando lugar al estándar IEEE 802.11b. Nokia y Symbol Technologies fundan la Wireless Ethernet Compatibility.

Alliance (WECA), conocida en la actualidad como Wi-FiAlliance, con el objeto de mejorar la difusión de las comunicaciones inalámbricas y asegurar la compatibilidad entre los equipos.

En Abril del 2000, WECA certifica la interoperabilidad de dispositivos para el estándar IEEE 802.11b, conocida desde entonces como el estándar WI-FI.

En la primera década del siglo XXI, el estándar IEEE 802.11 (WI-FI) permite que usuarios domésticos establezcan comunicaciones con otros computadores dentro de redes privadas pequeñas, y permite el acceso hacia la gran red.

Los dispositivos de red se vuelven cada vez más baratos, y el software involucrado en las conexiones tiene licenciamientos freeware. Estos factores dieron lugar al desarrollo de las primeras redes comunitarias en malla (MESH), con desarrolladores de software libre. (Sevilla Mesh, 2011).

El 3 de Junio en el 2006, en la Universidad de Cambridge, las redes MESH fueron usadas para el "StrawberryFair[1]" para distribuir televisión móvil, radio y servicios de Internet para un estimado de 80,000 personas.

En el año 2007, la milicia estadounidense desarrolló el Meraki, un mini router MESH inalámbrico, con una velocidad por encima de los 50 Mbps. El Meraki transmitía dentro del rango de frecuencias de radio del estándar 802.11; además su alcance fue optimizado para largas - distancias de comunicación, proveyendo coberturas sobre los 250 m.

[1] Festival local de música, espectáculos, artes y oficios. que se ha celebrado en Cambridge , Inglaterra , desde 1974

La Escuela Naval Posgraduada, Monterey CA, implementó una red inalámbrica MESH para la seguridad fronteriza. En el sistema piloto, cámaras satelitales retransmitían la señal de video, de alta definición, en tiempo real al personal en tierra a través de una red Malla.

EL MIT Media LAB[2] diseño el proyecto OLPC (One Laptop per Child), que entre otros objetivos, pretendía brindar acceso a internet a las escuelas en desventaja de los países en vías de desarrollo mediante redes MESH.

Así se garantizaba la implementación de una infraestructura robusta y barata. Según el plan, los computadores formaban parte de una red en malla, de tal manera que podrían acceder a internet siempre que hubiera algún computador cercano que pudiera actuar como nodo, y compartiera la conexión. (Sevilla Mesh, 2011).

La comunidad de Red Inalámbrica CUWIN (por sus siglas en inglés) desarrolla proyectos para la construcción de arquitecturas de redes inalámbricas comunitarias, rentables y eficaces.

En materia de enrutamiento, la CUWIN desarrollo el protocolo Hazy, un algoritmo que permite las computadoras comunicarse a través de la radio digital en una red de malla para reenviar mensajes a equipos que están fuera del alcance de contacto directo por radio.

Además, el Grupo de Redes Inalámbricas CUWIN (por sus siglas en inglés), en la Universidad de Illinois en Urbana-Champaign, están desarrollando un banco de pruebas de redes en malla inalámbrica multi-canal, multi-radio, denominado Net-X, como una prueba del concepto de aplicación de algunos de los protocolos de canales múltiples que se están desarrollando en dicho grupo. (Sevilla Mesh, 2011)

Las implementaciones se basan en una arquitectura que permite a algunas de las radios cambiar de canal para mantener la conectividad de red, e incluye protocolos para la asignación de canales y rutas.

---

[2] Laboratorio dentro de la Escuela de Arquitectura y Planificación en el Instituto de Tecnología de Massachusetts

SMESH es una red inalámbrica 802.11 multi-salto desarrollado por los departamentos Distributed System y Networks Lab en la Universidad Johns Hopkins.

Una red SMESH permite, mediante un esquema rápido de transferencia, que clientes móviles hagan roaming en la red sin ninguna interrupción en la conectividad, un rasgo apropiado para aplicaciones en tiempo–real, como VoIP.

Muchas redes MESH operan en múltiples bandas de radio. Por ejemplo, las redes MESH Firetide y Web Relay tienen la opción para comunicar nodo a nodo a 5.2 GHz o 5.8 GHz, y la comunicación entre nodo a cliente a solo 2.4 GHz (802.11). Esto es posible usando SDR (Radio Definida por Software, por sus siglas en inglés).

El proyecto Solar MESH examinó el potencial de suministrar energía a las redes 802.11-basado en MESH usando energía solar y baterías recargables. Los puntos de acceso estandarizados bajo la norma 802.11 resultaron ser inadecuados por su necesidad de mantener una alimentación continua.

Los esfuerzos de estandarización IEE802.11s consideran opciones de ahorro energía, pero las aplicaciones de energía solar podrían requerir nodos de radio individuales donde el ahorro de energía en los relés de enlace será inaplicable.

El proyecto ALA - Wireless MESH Network de la próxima generación de Internet ha desarrollado un set de algoritmos novel y protocolos para habilitar redes inalámbricas MESH como el estándar de la arquitectura de acceso para la siguiente generación de Internet.

Estándares recientes de comunicaciones cableadas han incorporado conceptos de Redes MESH. Un ejemplo es la ITU-T G.hn, un estándar que especifica una red de área local de alta velocidad (sobre 1 Gbps) que está usando el cableado de casa (Línea Eléctrica, líneas telefónicas y cables coaxiales).

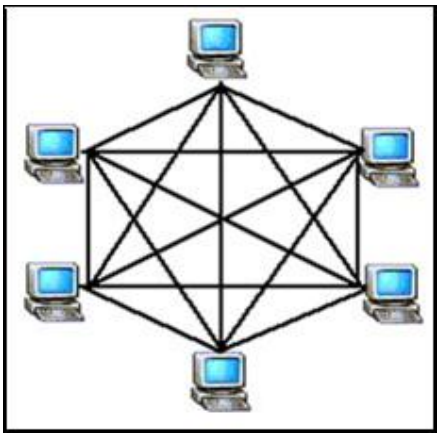
En ambientes ruidosos como líneas eléctricas (donde las señales pueden ser muy atenuadas y deterioradas por el ruido) es común que la visibilidad mutua entre los dispositivos de la red no se complete. En G.hn la retransmisión es realizada en la capa de Enlace de Datos. (Sevilla Mesh, 2011).

1.2. Definición de una red de topología MESH.

Una red de topología MESH es aquella que utiliza uno o inclusive varios arreglos de conexión. Se pueden definir dos tipos: topología parcial o total. En la topología parcial las conexiones se realizan solo con algunos de los demás nodos. En la topología Total las conexiones se realizan todos contra todos.

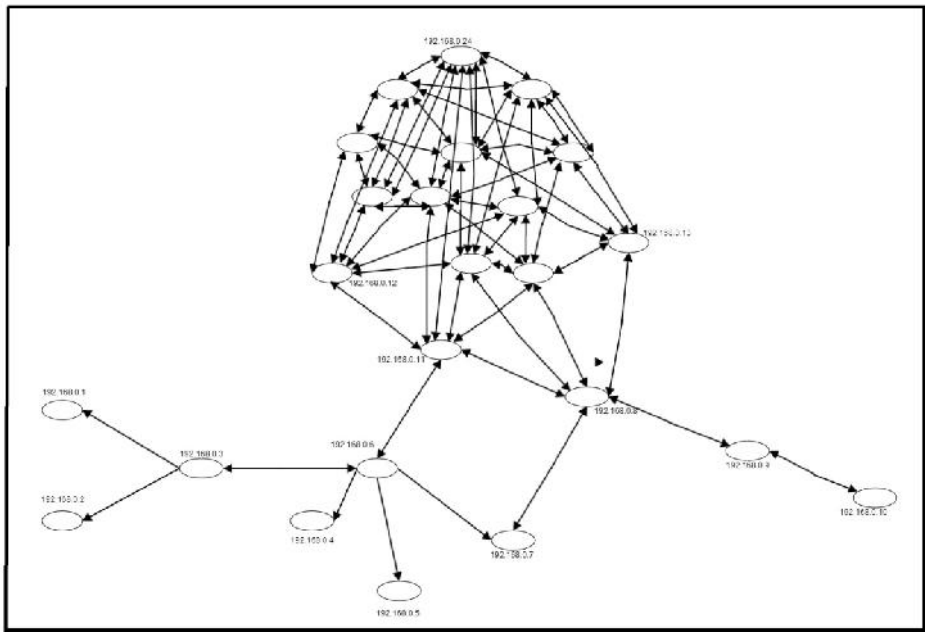
Esto queda mejor ilustrado en una red total simple, como se observa en la Figura 1, en la cual todos los nodos (computadores) están conectados a todos los demás.

Figura 1. Esquema de la red total.



Fuente: Sebastián Büttrich.less.dk wire

Figura 2. Diagrama de una red MESH parcial.



Fuente:Autor

En la Figura 2 se presenta una red compuesta por una red de topología parcial con una sección en topología total. En la topología parcial, un dispositivo está conectado solo con algunos de los dispositivos clientes de red, mientras que en un esquema de conexión total todos los dispositivos involucrados se conectan unos con otros.

1.2.1. Topología y dinámica de la red MESH.

En conexiones de redes inalámbricas el término “MESH” es usado a menudo como un sinónimo de “Ad hoc”, porque los nodos se conectan entre sí para establecer enlaces punto a punto. Una red MESH necesita de un software que gestione la red para establecer la comunicación entre todos los nodos.

Combinado con las dos tipos de la topología MESH y las capacidades de ad hoc, es una propuesta muy interesante.

Las implementaciones más exitosas de redes MESH han sido estáticas, por ejemplo los nodos, o las antenas colocadas en los techos de las casas, o edificios. Estas redes trabajan en un entorno dinámico, porque los terminales se conectan de forma móvil (red móvil), es decir que no permanecen estáticos, si no que tienen movilidad con respecto al que emite la señal inalámbrica por ejemplo: un router, un punto de acceso, o un repetidor de la señal; y estos están estáticos o fijos.

1.2.2. Red Ad - hoc.

Una red ad hoc es una red sin alambre, y descentralizada, porque no necesita de un punto de acceso central, sino que la comunicación de esta se establece por una conexión que depende de cada nodo y de esta manera conforma una ruta. En esta ruta se puede controlar la selección del camino para la seguridad del enlace, si uno falla, otro camino estará disponible para establecer la comunicación.

Como se puede apreciar, en esta definición cada nodo consecutivo depende sucesivamente del otro, esto quiere decir que el primer nodo se conectará con el segundo, y así sucesivamente hasta completar el enlace. Lo que no se puede hacer es conectar el cuarto con el segundo, no puede porque depende de su sucesión y es parcial.

El gran problema de estas redes es que se disminuye el ancho de banda mientras más conexiones tengamos, algo que se debe ser analizado con profundidad.

1.2.3. Definición del dispositivo NAT.

Un dispositivo NAT es un enrutador con dos puertos de red. El puerto externo utiliza una dirección IP enrutada globalmente, mientras que el puerto interno utiliza una dirección IP de uno de estos identificadores en grupos convenientes.

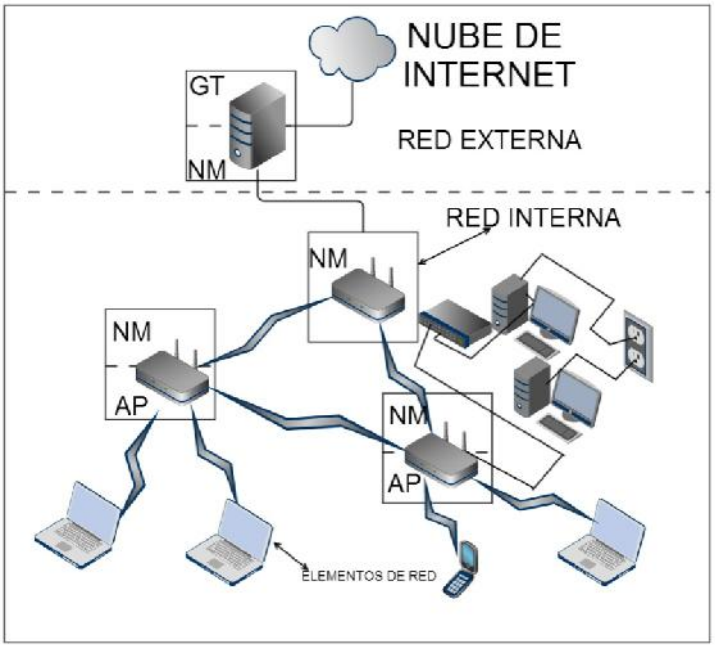
El enrutamiento mantiene un registro del lugar en la red donde están ubicados esos grupos. Los resultados del proceso de enrutamiento se guardan en una lista llamada tabla de enrutamiento. El reenvío es la acción de usar la tabla de enrutamiento para mandar un paquete a destino final o al "próximo salto" en la dirección a ese destino.

1.3. ELEMENTOS DE UNA RED DE TOPOLOGÍA MESH.

Básicamente los elementos de una red MESH Figura 3 se basan principalmente de su estructura determinada por dos tipos: 1) Elementos de red externa, 2) Elementos de red interna.

1.3.1. ELEMENTOS DE RED INTERNOS.

Figura 3. Elementos Red Interna, Externa.



Fuente:Autor

NODO MESH (NM)

En la Figura 3 se encuentra el Nodo MESH que es el responsable de establecer los paths de comunicaciones con el resto de nodos de la red y mantener las comunicaciones.

ACCESS POINT (AP)

La función más relevante de los Nodos MESH, es que nos dan la posibilidad de crear y gestionar la capa de servicio a los usuarios.

La estación base aparte de ser una estación (repetidor), tiene dos funciones: la de concentrador o hub de una red convencional en la que se conectan todos los terminales (Computadores con capacidad inalámbrica), implementando funciones de control; y la de conexión a la infraestructura cableada llevando a establecerse el puente (configuración de unión) con otras redes, como puede ser Internet.

MODO ETHERNET DE CONEXIÓN AP (GT).

En consecuencia, la estación base cuentaal menos con una conexión Ethernet 10/100 con posibilidad de funcionamiento en modo bridge transparente.

MODO GATEWAY DE CONEXIÓN AP (GT).

“En este modo gateway (con router +DHCP + NAT”) (García Fernández, 2006). Muchos de estos disponen opcionalmente de capacidad dealimentación por línea (in-line power) a través de la conexión Ethernet (PoE – Powerover Ethernet), lo que hace fácil su instalación, ya que su alimentación energética es a través del cable de red sin necesidad de hacer llegar corriente eléctrica por separado.

Al igual que el resto de estándar IEEE 802, el 802.11 se centra en las 2 capas inferiores del modelo OSI, la capa física y la capa de enlace.

• Capa Física:Espectro Ensanchado por secuencia directa (DSSS).
• Capa de Enlace (MAC): Adaptación de trama Ethernet + CSMA/CA (con Acknowledge).

El 802.11 define la arquitectura básica, características y servicios de 802.11b (García Fernández, 2006). La especificación 802.11b afecta solo a la capa física, aumentando la velocidad de transmisión y dotando de mecanismos para hacer la conexión más robusta.

Estos subcomités con el tiempo han sufrido cambios y modificaciones se enlista los siguientes:

- 802.11a: Hasta 54 Mbps en la banda de 5 GHz.
- 802.11b: Hasta 11 Mbps en la banda de 2.4 GHz (Wi-FI-b).
- 802.11g: Hasta 54 Mbps en la banda de 2.4 GHz.
- 802.11d: Control de acceso al medio (MAC).
- 802.11e: Para poder definir QoS (calidad de servicio).
- 802.11f: Protocolo entre Access Point (IAPP).
- 802.11h: Selección automática de frecuencias y control de potencia.
- 802.11i: Incremento de niveles de seguridad en las comunicaciones.
- 802.11n: Velocidad mejorada hasta 100-500 Mbps.

SOFTWARE DE GESTIÓN DE LA RED.

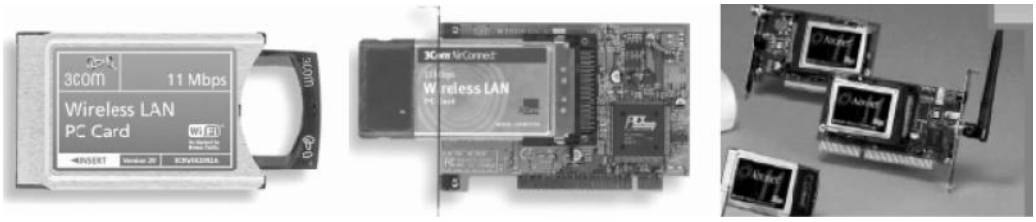
Por su característica de autoreparación es necesario un software de gestión que permita determinar la operatividad de los nodos. Debe permitir propagar a todos los nodos los cambios en las configuraciones. Mostrar las conexiones MESH establecidas entre los nodos.

1.2.1. ELEMENTOS FÍSICOS DE LA RED.

ADAPTADOR DE RED

Los adaptadores de red Figura 4 (uno por cada puesto establecido), adoptan el formato que es a cada terminal, (PCI, PCMCIA, PC Card, USB, utilizadas en portátiles, en PDA, antenas empotradas en postes). Implementan las funciones de estación, normalmente con antena integrada, permitiéndose configuraciones en modo ad- hoc o en modo infraestructura, y ahora con Linux en varios modos como: Master (Como Access Point), Managed (Administrador), Ad-hoc, Repetidor, y muchas más combinaciones. (García Fernández, 2006).

Figura 4. Adaptadores de Red Comunes.



Fuente: García Fernández.

COMPUTADORAS LAPTOP.

Son muy importantes debido a que cada una de ellas contiene la tarjeta inalámbrica.

ANTENAS EMPOTRADAS.

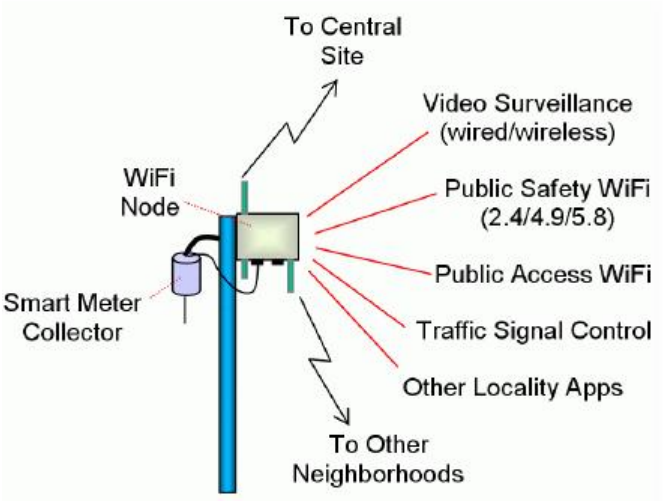
Estas van colocadas en paredes, postes eléctricos, y tienen cierta protección en contra de la lluvia, y ambientes dañinos. Alcanzan grandes coberturas y actúan como repetidores de la red MESH. Tienen dos tipos de frecuencia a 2.5 GHz, y 5 GHz.

ACCESO PÚBLICO WIFI.

Esto vendría por añadidura, ilustrado en la Figura 5, ya que es lo que se ofrece al usuario final, y está relacionado con la capa física del medio "MAC". Aparte de esto teniendo ya el acceso se dispone de los siguientes servicios:

- Control de la señal de tráfico.
- Video Vigilancia.
- Seguridad Pública WI-FI (2.4/4.9/5.8).
- Trasmisión de datos de alta velocidad (Video bajo demanda, Video de alta calidad de definición, telefonía IP, video Conferencia, IPTV, etc.
- Conectividad a varias localidades.
- Conectividad a otros vecindarios.

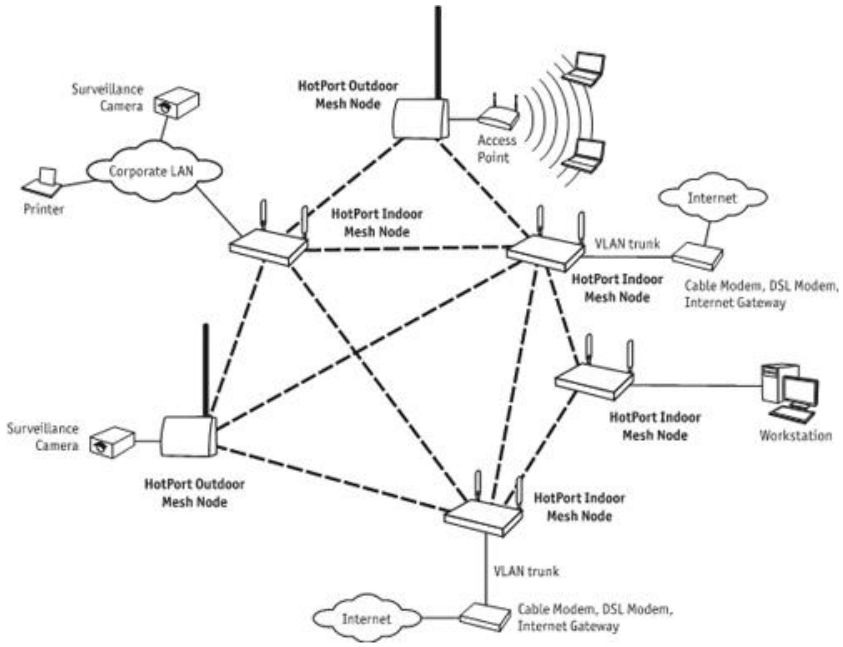
Figura 5. Elementos de Red Físico.



Fuente: Meshdynamics.com.

1.3.3. ESQUEMA COMPLETO DE UNA RED MESH.

Figura 6. Esquema de Red MESH completo.



Fuente: Manzano David.

“Los elementos que un usuario necesita para crear una red MESH son únicamente puntos de acceso (dispositivos de red wireless) Figura 6 funcionando en modo ad-hoc y al menos uno haciéndolo también en modo infraestructura para proporcionar acceso a Internet a todos los usuarios de la red”. (Manzano David, 2007).

Para tener más claro el asunto se menciona dos conceptos importantes el modo infraestructura, y el punto de acceso en modo ad-hoc.

En el modo infraestructura los puntos de acceso funcionan de forma equivalentealos hubs o concentradores, permitiendo que varios clientes wireless se comuniquenentre sí. A diario se utilizan varios puntos de acceso para cubrir unárea determinada como una casa, una oficina u otro tipo de área delimitada.

Los puntos de acceso poseen varias conexiones de red: latarjeta wireless y una o más tarjetas Ethernet que se utilizan para comunicarsecon el resto de la red.

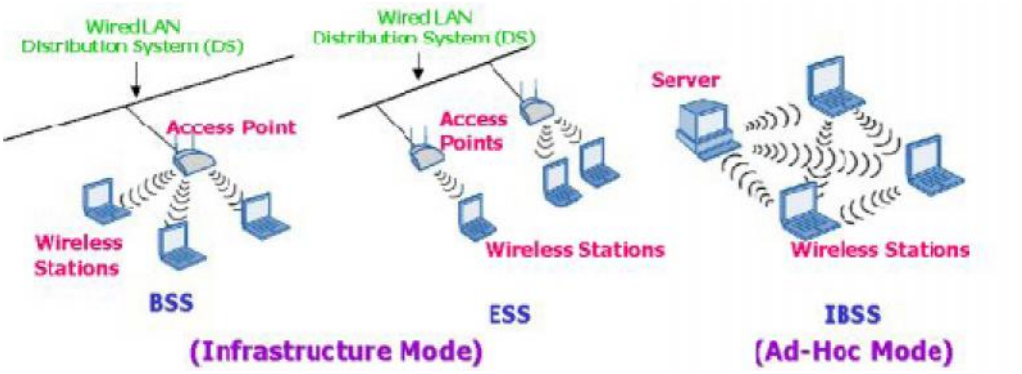
En el modo ad-hoc no existen conexiones entre los distintos puntos de acceso, de manera que cuando un dispositivo quiere comunicarse con otro lo hará con el que esté disponible y cerca de su rango de cobertura, actuando este como repetidor de la señal hasta llegar al dispositivo destino.

Las configuraciones ad-hoc son comunicaciones punto a punto. Aquí entra la función del protocolo de enrutamiento, que se encargará de encontrar un camino desde el dispositivo emisor hasta el dispositivo receptor sin congestionar la red.

Para que los dispositivos de una red funcionen en modo ad-hoc es necesario configurarlos para que operen en ese modo, accediendo, por ejemplo, a la interfaz web del punto de acceso, o al terminal de Linux, también es necesario que se encuentren en el mismo canal y ESSID.

En la Figura 7 podemos ver un ejemplo de cada uno de los modos de funcionamiento.

Figura 7. Modos de Infraestructura



Fuente: Manzano David.

Cada fabricante proporciona su firmware para administrar el punto de acceso. Actualmente encontramos muchas soluciones para proporcionar una mayor libertad de configuración a estos dispositivos y que permitirá a usuarios un poco más avanzados con el entorno Linux sacarle el máximo provecho al punto de acceso.

1.4. PROTOCOLOS DE LA RED MESH.

1.4.1. LISTA DE ALGUNOS PROTOCOLOS EXISTENTES.

Para el enrutamiento de paquetes a través de redes de malla existen los siguientes protocolos:

• AODV- Ad-Hoc on Demand Distance Vector (Vector Distancia a demandaAd hoc).
• B.A.T.M.A.N- Better Approach To Mobile Ad-hoc Networking (Mejor Aproximación a la red Móvil Ad hoc). (Wikipedia, 2012).
• Babel - a loop-free distance-vector routing protocol (protocolo a distancia-vector de protocolo de enrutamiento para IPv6 e IPv4 con propiedades de convergencia rápida).• DNVR - Dynamic Nix-Vector Routing.
• DSDV – Destination Sequence Distance Vector (Distancia Destino-secuencial - de enrutamiento de vector)
• DSR - Dynamic Source Routing (Fuente enrutamiento dinámico).
• HSLS - Hazy-Sighted Link State(Protocolo de enrutamiento basado en desechar los enlaces de baja calidad).

• IWMP - Infrastructured Wireless MESH Protocol (Infraestructura Protocolo de malla inalámbrica para redes de malla.De infraestructura por UFPB GRECO-Brasil).
• OLSR - Optimized Link State Routing protocol (protocolo de enrutamiento por optimización del estado del enlace).
• OORP - Order One Protocolo Routing (Orden Primero Protocolo Enrutamiento).
• OSPF - Open Shortest Path First(Basado en abrir primero la ruta más corta de enrutamiento).
• PWRP - Predictive Wireless Routing Protocol(predictivo Protocolo de enrutamiento inalámbrico).
• TORA - Temporally-Ordered Routing Algorithm(Temporal-Z Algoritmo de Enrutamiento).

1.4.2. DEFINICIÓN DEL PROTOCOLO D.S.D.V.

D.S.D.V (Destination Sequenced Distance Vector)

Este protocolo proactivo por definición está basado en tablas de encaminamiento y fue diseñado por Charles E. Perkins y Pravin Bhagwat. (Wikipedia, 2014).
El término proactivo hace referencia a un Sistema Adaptativo de encaminamiento basado en el intercambio de paquetes de control. Continuamente se actualiza la información de accesibilidad en las tablas de encaminamiento de los nodos.

La Ruta está inmediatamente disponible cuando se solicite. El Ancho de banda sustancial se utiliza para el control de tráfico grande.

1.4.3. FUNCIONAMIENTO DEL PROTOCOLO D.S.D.V

"El enrutamiento de un protocolo basado en vector de distancias requiere que un router informe a sus vecinos de los cambios en la topología periódicamente y en algunos casos cuando se detecta un cambio en la topología de la red". (Wikipedia, 2014).
Comparado a los protocolos de estado de enlace, que necesitan que un router informe a todos los nodos de una red acerca de los cambios en su topología, los algoritmos de vector de distancias tienen mucha menos complejidad computacional.
Además, las principales características de los diferentes algoritmos VD (vector de distancias) son siempre las mismas. El algoritmo VD se basa en calcular la dirección y la distancia hasta cualquier enlace en la red.

El costo de alcanzar un destino se lleva a cabo usando cálculos matemáticos como la métrica del camino. RIP cuenta los saltos efectuados hasta llegar al destino mientras que IGRP utiliza otra información como el retardo y el ancho de banda.

Figura 8. Esquemas de Distancias de los Routers.

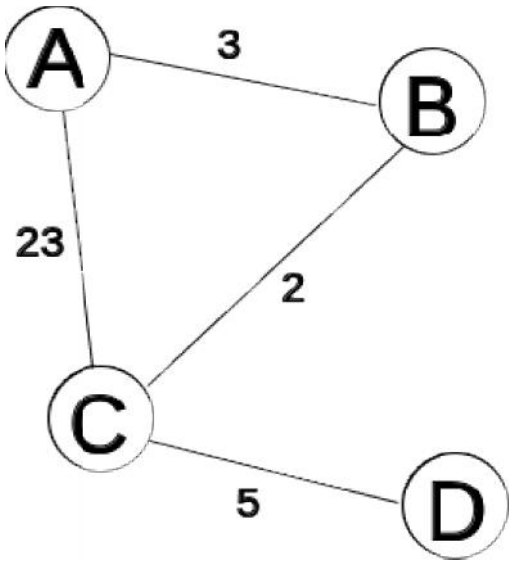
"Los cambios son detectados periódicamente ya que la tabla de enrutamiento de cada router se envía a todos los vecinos que usan el mismo protocolo. Una vez que el router tiene toda la información, actualiza su propia tabla reflejando los cambios y luego informa a sus vecinos de los mismos". (Wikipedia, 2014).

Este proceso se conoce también como "enrutamiento por rumor" ya que los nodos usan la información de sus vecinos y no pueden comprobar si ésta es verdadera o no.

El algoritmo de Bellman-Ford se adapta perfectamente al modo de aprendizaje de los nodos que "nacen", es decir, cuando se conectan a la red.

A medida que el algoritmo progresa, el nuevo nodo va adquiriendo más información sobre el resto de nodos de la red. Este algoritmo converge rápidamente cuando se conectan nuevos nodos. Por ello se suele decir que las buenas noticias viajan rápido por la red. Figura 8.

Figura 8. Esquemas de Distancias de los Routers.



Fuente: Wikipedia

En la Figura 9 empezamos calculando las matrices de distancias para cada router. El "camino más corto" está marcado con el color verde, un "camino más corto" nuevo está indicado en amarillo.

Figura 9. Tabla de valores de costo de los Routers.

T = 0

desde A	vía A	vía B	vía C	vía D
a A				
a B		3		
a C			23	
a D				

desde B	vía A	vía B	vía C	vía D
a A	3			
a B				
a C			2	
a D				

desde C	vía A	vía B	vía C	vía D
a A	23			
a B		2		
a C				
a D				5

desde D	vía A	vía B	vía C	vía D
a A				
a B				
a C			5	
a D				

T = 1

desde A	vía A	vía B	vía C	vía D
a A				
a B		3	25	
a C		5	23	
a D			28	

desde B	vía A	vía B	vía C	vía D
a A	3		25	
a B				
a C	26		2	
a D			7	

desde C	vía A	vía B	vía C	vía D
a A	23	5		
a B	26	2		
a C				
a D				5

desde D	vía A	vía B	vía C	vía D
a A			28	
a B			7	
a C			5	
a D				

T = 2

desde A	vía A	vía B	vía C	vía D
a A				
a B		3	25	
a C		5	23	
a D		10	28	

desde B	vía A	vía B	vía C	vía D
a A	3		25	
a B				
a C	26		2	
a D	31		7	

desde C	vía A	vía B	vía C	vía D
a A	23	5		33
a B	26	2		12
a C				
a D	33	9		5

desde D	vía A	vía B	vía C	vía D
a A			10	
a B			7	
a C			5	
a D				

T = 3

desde A	vía A	vía B	vía C	vía D
a A				
a B		3	25	
a C		5	23	
a D		10	28	

desde B	vía A	vía B	vía C	vía D
a A	3		7	
a B				
a C	8		2	
a D	31		7	

desde C	vía A	vía B	vía C	vía D
a A	23	5		15
a B	26	2		12
a C				
a D	33	9		5

desde D	vía A	vía B	vía C	vía D
a A			10	
a B			7	
a C			5	
a D				

Fuente: Wikipedia

Como se puede observar el Verde es el camino más corto y el amarillo es otro posible camino más corto también.

1.5. ARQUITECTURA DE LA RED DE TOPOLOGÍA MESH.

1.5.1. Infraestructura del Sistema

La infraestructura utiliza para el buen funcionamiento del sistema un equipo, dónde seubicará la aplicación central (Software de Gestión) Figura 10, con sistema operativo Linux y con una tarjeta wireless. (Alférez Antonio, 2006).

Este equipo tendrá que formar parte de una red MESH, esto no implica que deba estar permanentemente dentro de la red, pero debe estar,a la hora de administrar los dispositivos que forman parte de ella.

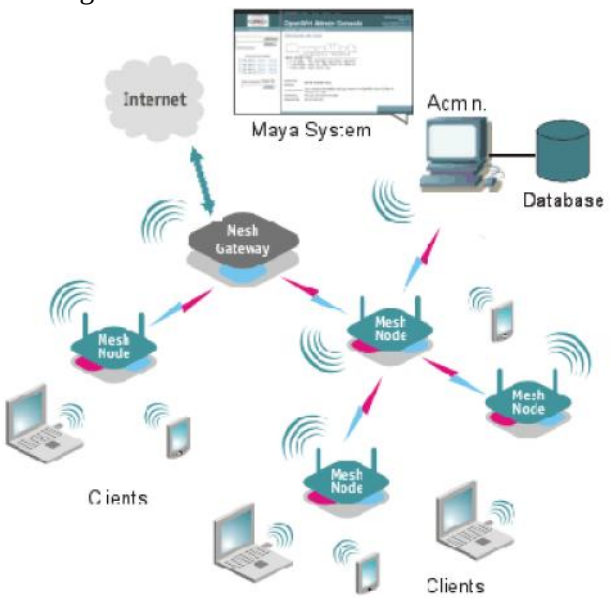
Un mismo equipo, por ejemplo un portátil, puede administrar todas las redes que se desee, mientras los dispositivos de esa red estén configurados para esto(y tenganinstalado el software) y el equipo pertenezca en ese momento a dicha red, y por su-puesto que obtenga los permisos necesarios para administrarla Figura 10.

El otro componente básico para nuestra infraestructura son los puntos de acceso.

Todos ellos deberán estar funcionando en modo ad-hoc y correctamente configurados.

En resumen, la aplicación en sí se instalará en el punto de control y en los puntos de acceso será necesario el uso de un software muy reducido para comunicarse con el punto de control, además de una serie de configuraciones que se explicarán con todo detalle en el apéndice del documento.

Figura 10. Arquitectura global del sistema.



Fuente: Manzano David.

1.5.2. Lenguajes Utilizados

Los lenguajes de programación más usados en estos proyectos han sido variados en función de las necesidades y de las limitaciones que implica programar para dispositivos como los puntos de acceso que cuentan con un espacio de almacenamiento mucho menor y un número de herramientas más reducido que un computador normal. A continuación enumeraremos los lenguajes más relevantes que son utilizados en la actualidad. (Alférez Antonio, 2006).

1. HTML: Lenguaje esencial para de creación de una página web. Esta desarrollada en una página web y permite estructurarla.

2. CSS: Las hojas de estilo en cascada son un lenguaje formal usado para definir la presentación de un documento estructurado escrito en HTML. Esto dará simplicidad al trabajo a la hora de crear la apariencia de la aplicación.

3. PHP: Es un lenguaje de programación interpretado se utiliza entre otrascosas para la programación de páginas web activas, y se enfatiza por sucapacidad de con el código HTML.

4. Java Script: Es un lenguaje interpretado orientado a las páginas web, con una sintaxis parecida a la del lenguaje Java.

5. SQL SERVER: Es un lenguaje declarativo de acceso a bases de datos relacionales. Se encargará de mantener la información sobre los puntos de acceso en la base de datos, dónde se realizan consultas y actualizaciones desde el código PHP.

6. El lenguaje C esuno de los más comunes de programación. Se utilizó para desarrollar pequeñas aplicaciones para los puntos de acceso dadas las características de ambos; el hecho de no ser un lenguaje de alto nivel, proporcionamayor carga al dispositivo.

7. Shell Script: Son programas escritos con comandos UNIX. Todas las opcionesde cambio de parámetros en los dispositivos que ofrece la herramientaestán implementadas en Shell Script.

8. OTCL: (Tool Comand Lenguage) Es una extensión de la Herramienta de Comando de Control, este tipo de programación es la escogida debido a que es orientada a objetos en un Scrib, este es un archivo con extensión tcl, el cual es el encargado de tener los comandos para el funcionamiento del protocolo de enrutamiento y la simulación que se propuso hacer aquí se pone todo: posicionamiento de los nodos, cobertura, cálculos de potencias, trasmisión de los nodos, tiempos de simulación, restricciones programables, etc.

1.6. Aplicaciones.

Por ejemplo: en un ambiente difícil como una situación de emergencia, túneles, las plataformas petroleras, campo de batalla de vigilancia, video móvil de alta velocidad, aplicaciones en el transporte público o tablero en tiempo real de la telemetría del coche de carreras. Una importante aplicación posible para redes inalámbricas MESH es VoIP. Usando una escena de calidad de Servicio, las redes MESH inalámbricas pueden soportar llamadas de telefonía local para ser ruteadas para alcanzar la MESH.

Algunas aplicaciones concurrentes son:

- Fuerzas militares están ahora usando redes inalámbricas MESH para conectarse sus computadoras, principalmente ordenadores robustos, en campus de operaciones.
- Los medidores eléctricos que se han desplegado en residencias de la transferencia de sus lecturas de uno a otro y, finalmente, a la oficina central para la facturación sin necesidad de lectores de medidores humanos o la necesidad de conectar los medidores con cables.
- El satélite - 66 de constelación Iridio funciona como una red de malla, con enlaces inalámbricos entre satélites adyacentes. Las llamadas entre dos teléfonos vía satélite se enrutan a través de la malla, de un satélite a otro a través de la constelación, sin tener que pasar por una estación terrena. Esto hace que para un recorrido más pequeño de la señal, lo que reduce la latencia, y también permite la constelación de operar con las estaciones terrenas mucho menos que si serían necesarios 66 satélites de comunicaciones tradicionales.
- Por último aplicable para todas las Universidades paralos estudiantes de todas las facultades que necesitan conectarse al mismo tiempo.

CAPÍTULO 2

ANÁLISIS DE LA RED DE TOPOLOGÍA MESH.

2.1. Análisis Técnicos de los Elementos de esta Red.

Teniendo el hardware (físico) se necesitará hacer la construcción de una red, hay muchas variantes en lo referente a productos y complementos. Empresas como Atheros, Broadcom, Linksys o RealTek son los principales fabricantes de chipsets que utilizan diferentes puntos de acceso para el mercado.

Son numerosos los fabricantes y modelos de estos dispositivos, en la Figura 11 podemos observar las características de los más selectos debido a que son aptos y compatibles con OpenWrt y la plataforma Linux.El que es el más utilizado y recomendado por expertos y usuarios, el WRT54GL fabricado por Linksys, que permite interconectar varios ordenadores mediante enlaces Ethernet 802.3 y 802.11g inalámbricas.

Figura 11. Linksys WRT54GL

Fuente: Manzano Gonzáles.

"El modelo WRT54GS es prácticamente idéntico, excepto por el aumento de memoria RAM y la incorporación de la tecnología SpeedBoost (Mayor velocidad).Este router es único entre los dispositivos de consumo doméstico, debido a que los desarrolladores de Linksys tuvieron que liberar el código fuente del firmware del router para cumplir con los requerimientos de la GNU GPL". (Manzano David, 2007).

Este suceso brinda posibilidades a los entusiastas de la programación para modificar el firmware y así añadir o cambiar las funcionalidades del dispositivo.

Existen varios proyectos de desarrollo que proveen versiones mejoradas del firmware para el WRT54G, como el OpenWrt y otros como: Batbox o HyperWRT.
Y ha servido de base para el desarrollo de numerosas comunidades wireless, como la mencionada FON.

El WRT54GL original estaba equipado con una CPU MIPS a 125 MHz con 16 MB de memoria RAM y 4 MB de memoria flash para almacenar el firmware.

En revisiones posteriores, se aumentó la velocidad de la CPU a 200 MHz y se duplico tanto la memoria RAM como el flash a 32 y 8 MB, respectivamente.

Todos los modelos vienen con un switch de 5 puertos (el puerto para Internet está en el mismo switch, pero en una VLAN diferente) y con un chipset inalámbrico de Broadcom, Intersil, Atheros, etc.Igualmente, dispone de dos antenas externas conectadas a través de conectores de polaridad inversa TNC.

Hay que aclarar que la versión del WRT54G (la versión 5) no aceptará firmware de terceros dado que el sistema ya no corre sobre Linux, desde hace poco tiene firmware deterceros como DD-WRT.

2.2.1. Hardware Linksys

Alimentación

Todas las versiones del WRT54G requieren la misma alimentación de 12V DC. 1A, exceptuando la versión 1.0, con su fuente de poder de 5V DC 2A, esto debido, a que esta primera versión de la serie contaba con la compatibilidad de PoE (Power over Ethernet) en donde la fuente de alimentación proviene de los pares de cable no usados del cable de Ethernet. (Linksys, 2014).

Arquitectura del Procesador

Toda la serie WRT54G implementa procesadores Broadcom MIPS (Microprocessor without Interlocked Pipeline Stages), que cuentan con RISC (Reduce Instruction Set Computer), es decir un set de instrucciones reducido, en el cual el tiempo de ejecución de las mismas es menor, y donde también se disminuye el número de accesos a la memoria. (Linksys, 2014).

Es importante señalar que la mayoría del software libre basado en Linux como es el caso del WRT54G está hecho para la plataforma Intel x86, que implementa otra arquitectura basada en un set de instrucciones más complejos CISC (Complex Instruction Set Computing), de la que desciende la mayoría de procesadores de computadores de escritorio.

Debido a lo anterior se hizo necesario la incursión de un Cross Compiler, el cual es un compilador capaz de crear código ejecutable para una plataforma diferente a la que se está corriendo, esto con el fin de que el firmware sea soportado por el procesador del Router. (Linksys, 2014).

El enrutador WRT54G se compone principalmente de 3 funciones, el procesamiento, control de acceso al medio de Ethernet (Ethernet MAC), y MAC del wireless.

A través de los distintos lanzamientos de la serie WRT54G, se observa la implementaciónde dos familias de procesadores Broadcom: BCM47xx y BCM5352.

BCM47xx: esta serie está compuesta por dos versiones, el BCM4704 en el cual este integrado solo cumplía la labor de procesamiento con una velocidad de reloj de 125MHz, mientras que el chip Broadcom BCM2050 se encarga del radio wireless, por otra parte, inicialmente el procesador ADMTec ADM6996 se encargó de la MAC de Ethernet, adelante en la versión 2.2 del Router ser reemplazado por el chip Broadcom BCM5325.

Con la inclusión de la versión BCM4712 se incluyó en un solo integrado la CPU y la MAC del wireless con el sistema SoC (System on a Chip), manteniendo por separado en esta familia el integrado de la MAC de Ethernet, además de incrementar la velocidad de procesamiento a 200 MHz.

La segunda familia de procesador, el Broadcom BCM5352 hizo su primer aparición en la versión 4.0 del Router, en la que su principal novedad fue la inclusión de la nueva generación de la arquitectura SoC, ya que incorporo las 3 funciones de CPU, MAC del Ethernet y wireless MAC en solo integrado, manteniendo la velocidad del procesador en 200MHz. (Linksys, 2014).

Almacenamiento.

La capacidad de almacenamiento como parte fundamental del funcionamiento del dispositivo, ya que es ahí donde se almacena todo el software del equipo, es decir el firmware, está a cargo del tipo de memoria no volátil, específicamente de memoria flash, siendo las versiones 1, 2 y 3 del WRT54GS las de mayor capacidad con 8MB.

La versión Linksys WRT54GL que fue seleccionada en esteestudio tiene una capacidad de memoria de 4MB.

Memoria RAM.

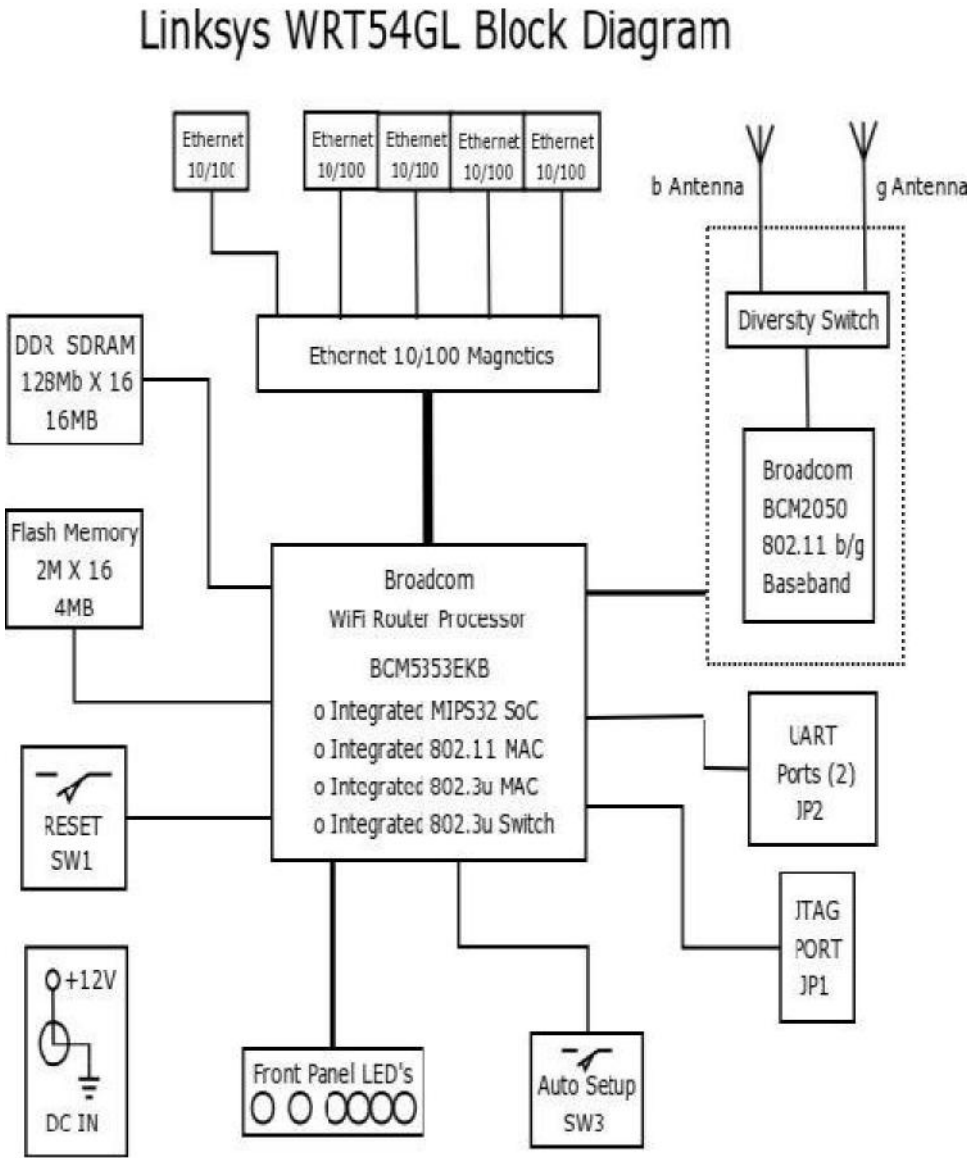
Los modelos del router WRT54G usan memoria SDRAM (Synchronous Dynamic Random Access Memory), es decir memoria RAM de acceso síncrono que se conecta al reloj del sistema, con la capacidad de leer o escribir a un ciclo de reloj por acceso sin estados de espera intermedios. Esta memoria esta soldada directamente sobre la tarjeta principal con una capacidad de 16 MB en la versión inicial del router.

Serie LINKSYS WRT54G

El firmware linksys WRT54G se basó en Linux y este código fuente fue liberado para cumplir con la licencia GNU GPL, dando la oportunidad a terceros de modificar y crear funciones extras, para lo cual la compañía llevó a lanzar el WRT54GL, versión que fue creada para facilitar el “Hacking”. Esta versión permite retirar las antenas, tiene amplio espacio en la PCB para adaptar un cable tipo JTAG en caso de daño al firmware, con el cual se puede poner un cable serial y aumentar la memoria externa. (Linksys, 2014).

Como se observa en la siguiente Figura 12 el Router WRT54GL donde está el Diagrama de Bloques del Router escogido se puede apreciar el integrado SoC (System-on-Chip), tiene según lo que se en este 5 puertos Ethernet 10/100, el diversity chip y la memoria. Este router carga un Firmware que se grava en la memoria RAM de este.

Figura 12. Diagrama de Bloques Linksys WRT54GL



Fuente: Linksys.

Firmware.

El firmware es un bloque de instrucciones con un fin específico y directamente ligado a un hardware, se encuentra en memoria no volátil y es el encargado de controlar a más bajo nivel el hardware, en otras palabras este funciona de interfaz entre el hardware y el software, un ejemplo de firmware es el que se monta sobre la BIOS de un computador y sobre este se soporta el sistema operativo. (Linksys, 2014).

Tabla 1. Tabla de Puntos de accesos más destacados

Fabricante	**Modelo**	**Plataforma y Frecuencia**	**Flash**	**RAM**	**Wireless NIC**	**Precio**
Buffalo	WZR-RSG54	Broadcom 4704@266MHz	8MB	64MB	Broadcom (mini-PCI)	$199
Mikrotik	Crossroads	MIPS32 4KEcbasado 184MHz	8MB	32MB	MIPS32	S/v
Linksys	WRT54GL	CPU MIPS a 125 MHz	4MB	16MB	MIPS	$69.47

Fuente: Autor.

Como se observa en la Tabla 1 el precio del Linksys WRT54GL es el más barato comparado con el Buffalo de $199. Por su costo se eligió este debido a que cumple con las condiciones técnicas que ya vimos antes aparte de tener un precio bajo de $69.47 comparado con uno de los más caros.

2.2. Software´s importantes para la construcción de la red.

Wifidog

Un software interesante puede ser el que proporciona Wifidog. Se trata de un proyecto que proporciona una solución empotrable y completa para el uso de un captive portal dentro de una comunidad wireless o para personas que quieren compartir su punto de acceso y desean evitar que se produzcan abusos de su conexión a internet.

Wifidog fue diseñado para tener la opción de tener un control de centralizadodel acceso, reparto del ancho de banda de cada cuenta, lista de nodos activos einformación específica de cada punto de acceso y cada cliente.

Este no se basa en Java Script, y funciona en cualquier plataforma con un navegador, incluso en teléfonos móviles, o en PDAs. Está escrito en C para que sea sencilla la instalación en sistemas empotrados. Se ha diseñado exactamente para el Linksys WRT54G usando OpenWrt, y además funciona en cualquier plataforma Linux de actualidad). Su capacidad de almacenamiento de estos dispositivos es muy mínima acerca de los 30 KB). (Lugro Mesh, 2010).

Como se puede apreciar que pequeña cantidad de almacenamiento ocupa, cada vez estos software son mejorados y optimizados en su tamaño, aparte de que dan grandes avances acoplándose a nuevas tecnologías de los enrutadores.

El captive portal Wifidog contiene: un Gateway, y un servidor de autenticación; el servidor de autenticación está elaborado en PHP con base de datos en PostgreSQL y permite autenticar clientes en un entorno captive portal (Pagina web de acceso para varios usuarios).

Desde aquí el administrador podrá manejar las cuentas de usuario, estadísticas y podrá revisar las características específicas de cada usuario mediante los logs almacenados.

El gateway será el encargado de conectarse al servidor de autenticación para comprobar si debe aceptar o denegar el acceso a un determinado usuario.

Nightwing

Nightwing, permite la creación de redes wireless MESH, que han tenido éxito en comunidades, realizando configuraciones fáciles con el objetivo de hacer más fácil y entendible su software. Utiliza una implementación de tecnología MESH denominada B.A.T.M.A.N, que ya le mencionamos anteriormente y que permite que se extienda una red Wireless con la simplicidad de agregar equipos y que funcione con la mínima intervención humana. (Lugro Mesh, 2010).

El problema de este software es que tendríamos que comprar los routers que tengan implementado esta tecnología para hacerlo tan simple, debido a que se implementa bajo software compatibles a su tecnología, es decir los enrutadores normales no tienen esta compatibilidad con Nightwing.

Nightwing contiene varios software importantes y entre estos tenemos los siguientes:

- **WiFiDog**

Uso actual: En Nightwing es el portal cautivo utilizado, contiene el componente llamado Gateway. También se utiliza el Servidor de Autenticación.

- **Dnsmasq**

Descripción: Dnsmasq es un servidor de DNS y servidor de DHCP, liviano y fácil de configurar. Está diseñado para proveer DNS y opcionalmente DHCP, a una red pequeña. Puede servir los nombres de máquinas locales que no están en el DNS global.

"El servidor de DHCP se integra con el servidor de DNS y permite máquinas con la opción de obtener dirección de IP por DHCP aparecer en el DNS con el nombre configurado tanto en cada host o en un archivo central de configuración". (Lugro Mesh, 2010).

Uso actual: En Nightwing como servidor local de DNS y servidor local de DHCP.

- **OpenWrt**

Uso actual: Distribución GNU/Linux base para el desarrollo de Nightwing.

- **OpenDNS**

Descripción: "OpenDNS es un servicio gratuito de resolución de DNS para consumidores y negocios ofrecido como una alternativa para usar los servicios de DNS del proveedor del servicio de Internet". (Lugro Mesh, 2010)

Al instalar los servidores de OpenDNS en locaciones estratégicas y empleando un gran cache (memoria) de nombres de dominios, las consultas de DNS son usualmente procesadas más rápido, por lo que se acelera la recepción de la velocidad de las páginas web.

Por lo que el aumento esta no es siempre notorio en cada solicitud, pero sólo con solicitudes que no están almacenadas en el caché local (memoria local).
OpenDNS permite la posibilidad de utilizar otras características como el bloqueo de sitios web para adultos, la protección contra phishing (hacker de tu cuenta).

Uso actual: Como servidor externo de DNS y como herramienta de filtrado de contenido.

- **Netfilter/IPTables**

Descripción: Netfilter es un framework disponible en el kernel Linux que permite interceptar y manipular paquetes de red. (Lugro Mesh, 2010).

Este framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. El componente más conocido es el firewall que filtra paquetes, pero también se utiliza para realizar otras tareas como la traducción de direcciones de red (NAT). Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos (firewalls) basados en Linux.

"El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías". (Lugro Mesh, 2010).
IPTables es el nombre de la herramienta de espacio de usuario por lo cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.
El nombre IPTables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter.

Sin embargo, el proyecto ofrece otros subsistemas independientes de IPTables tales como el connection tracking system (sistema de seguimiento de conexiones), o Queue, que permite encolar paquetes para que sean tratados desde espacio de usuario. IPTables es un software disponible prácticamente en todas las distribuciones de GNU/Linux actuales.

Uso actual: Para el filtrado, el rastreo de conexiones, traducción de direcciones de red (NAT).

OpenWrt

"OpenWrt es una distribución de Linux para sistemas empotrados" (Manzano David, 2007).

Al remplazar el firmware tradicional estático que nos da el proveedor, por un software de un sistema totalmente configurable. Esto da libertad al usuario en las aplicaciones y configuraciones que el vendedor soporta y es una oportunidad para personalizar el dispositivo mediante el uso de extensiones (paquetes de instalación), permitiendo una funcionalidad muy opcional a nuestro punto de acceso.

Una ventaja de OpenWrt es que nos da la posibilidad de tener muchas herramientas para ser instaladas (todas aquellas se reducen al tamaño físico de la memoria de un router), por ejemplo, servidor SNMP para obtener datos estadísticos, información del dispositivo; TCPDUMP, que sirve para examinar los paquetes que circulan por la red o IPTables, que se conoce como el firewall de Linux, se tiene en cuenta también la gran variedad de librerías como las del OpenSSL y bastantes utilidades.

Una virtud más es que OpenWrt ofrece un framework para construir una aplicación sin tener que construir el firmware por completo, esto da a los usuarios una personalización y bastantes formas de usar el dispositivo. (Manzano David, 2007).

Teniendo esto en cuenta esto un pequeño sistema instalado en la memoria de un router nos brinda la ventaja de ahorrar el espacio de almacenamiento y permite realizar nuestras propias aplicaciones, algo que no se puede con el firmware de fábrica.

Siendo así, el entorno de desarrollo de aplicaciones que ofrece OpenWrt, es dar utilidades como el compilador cruzado, para la compilación de código (como C o C++) desde nuestra arquitectura (la i386) a la arquitectura del dispositivo (MIPS).

OpenWrt tiene una interfaz web para la configuración de los parámetros más importantes, los usuarios principiantes no tendrán ningún problema de acople a esta utilidad. Habría que analizar los beneficios que nos da OpenWrt, ya que es el más efectivo por comandos SSH, se puede también manejar los dispositivos.

Sabiendo que se puede cambiar los parámetros por línea de comandos que serán básicas para una red MESH, y para eso tenemos que instalar un protocolo de enrutamiento, este es el responsable de establecer el lenguaje de comunicación entre terminales-puntos de control. (Manzano David, 2007).

La idea es tener un punto de control que gestione todos los puntos de red, acompañado de un lenguaje de conexión entre nodos, para esto tienen que estar bien configurados, y quizá la misma versión del software, también los dispositivos funcionando en modo ad-hoc y en modo infraestructura para que nuestro sistema funcione.

Existen varios protocolos de red para una red de topología MESH, entre estos los más destacados son: OLSR, D.S.D.V.

Teniendo esto en consideración al estar ya configurada la parte ad-hoc de la red MESH, un grupo de puntos de acceso distribuidos físicamente para ofrecer cobertura a usuarios que se deseen conectarse a la red. Un paso básico para la creación de la red MESH es proporcionar acceso a Internet, para lo cual, al menos un punto de acceso que forma la red deberá estar en modo infraestructura y el resto en modo ad-hoc para encaminar los paquetes de la red ad-hoc y viceversa. (Manzano David, 2007).

En el caso de salida de paquetes de la red hacía internet deberá desechar las cabeceras del protocolo de encaminamiento para que la información viaje por internet, y en el caso inverso deberá añadirlos, para que la información llegue al nodo de la red Ad-hoc.

2.3. Procedimiento para el análisis de costos.

2.3.1. Durabilidad Económica

La durabilidad económica es un tema muy interesante, ya que en muchas empresas es un factor importante especialmente en las públicas, y privadas. Al mencionar durabilidad me refiero a un sistema que se construye para permanecer indefinidamente.

El tiempo que debe permanecer es de un periodo de 5 años o más. Este tiempo es el esperado para las infraestructuras de TIC y tecnologías inalámbricas.

Muchos suponen que hay un modelo comercial que va a funcionar para todas las comunidades, y que la clave del éxito es encontrar esa solución tipo “Comercial”.

En la práctica no es así. Cada comunidad, pueblo o aldea son diferentes. No hay modelo prescrito que satisfaga las necesidades de todas las zonas de países en desarrollo.

A pesar de que algunos lugares sean semejantes en términos económicos, las características de un modelo comercial sostenible varían de comunidad en comunidad. A pesar de que un modelo funcione en un poblado, otro poblado cercano puede no tener las características necesarias para que el mismo modelo sea durable.

En estas situaciones, otro modelo debe diseñarse para adaptarlo al contexto de esta comunidad en particular. (Flickenger Rob, 2008).

2.3.2. Pequeñas pautas para arrancar el estudio.

Para crear la red de topología MESH en la Universidad del Azuay, en la Facultad de Ciencia y Tecnología se quiere lograr que los nodos conectados que brindan cobertura de red inalámbrica puedan ser gestionados individualmente, para lo cual se necesita permisos en la parte de la administración de la Universidad, para controlar el ancho de banda, registros de conectividad que cada usuario utilice, con el objetivo de mejorar la cobertura y dar un ancho de banda que no exceda el límite permitido para distribuir equivalentemente este. (Flickenger Rob, 2008).

El primer paso incluye la conformación de esta visión con el estímulo proveniente del equipo completo o del personal.

El propósito es brindar mejor cobertura de red inalámbrica a la Universidad del Azuay en la Facultad de Ciencia Y Tecnología.

Al gestionar los nodos que brindan cobertura de red se puede ahorrar en enrutadores y obtener así una mejor topología de red y minimizar los costos por enrutador.

Los reactores principales de la red son: Los Enrutadores, el Backbone de la Universidad, cables, espectro electromagnético, licenciamientos delos programas, servicios de internet por ISP.

2.3.3. Los marcos regulatorios para sistemas inalámbricos.

Primero, se investiga si cualquier organización tiene el derecho de usar frecuencias de 2,4 GHz sin licencia. En la mayoría de los casos la banda de 2,4 GHz es de uso libre en todo el mundo; sin embargo, en algunos países el uso de esta banda está restringido, ola licencia para su uso es muy costosa. “Por ejemplo, a pesar de que las redes inalámbricas son legales en Ucrania, el gobierno exige una licencia muy cara para usar las frecuencias de 2,4 GHz, lo que hace que su utilización sea prohibitiva”. (Flickenger Rob, 2008).

Lo más frecuente es que sólo Proveedores de Servicio de Internet bien establecidos tengan el flujo de dinero suficiente para pagar estas licencias.En estos casos la falta de flujo de dinero es un obstáculo para una comunidad pequeña que quiera compartir una red inalámbrica con otros socios u organizaciones.

En el Ecuador, son un poco asequibles: como no hay tantas restricciones para el uso de redes inalámbricas, la posibilidad de compartir la conexión a Internet en zonas de Campus Universitarios son posibles dentro de las Frecuencias 2.8 GHz y 5.0 GHz, pero si hay una interferencia con el espectro radioeléctrico no hay como hacer reclamos a lo menos si estamos en ambientes exteriores, más no en los ambiente interiores.

Lo prohibitivo según las normas es más si se quiere lucrar en ese caso se necesita tener un título que permita negociar con los servicios de Telecomunicaciones.

Artículo 1 Ámbito de la ley.- La presente ley especial de Telecomunicaciones tiene por objeto normar en el Territorio Nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos, e información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas el ectromagnéticos.

Los términos técnicos de telecomunicaciones no definidos en la presente Ley, serán utilizados con los significado establecidos por la Unión Internacional de Telecomunicaciones.

Artículo 2 menciona Espectro Radioeléctrico. Diciendo que este pertenece al Estado su control, administración.

Artículo 10 mencionado en la ley especial de Telecomunicaciones Reformada del Ecuador dice "No será necesaria autorización alguna para el establecimiento o utilización de instalaciones destinadas a intercomunicaciones dentro de residencias, edificaciones e inmuebles públicos o privados, siempre que para el efecto no se intercepten o interfieran los sistemas de telecomunicaciones públicos. Si los hicieran, sus propietarios o usuarios obligados a realizar, a su costo, las modificaciones necesarias para evitar dichas interferencias o intercepciones, sin prejuicio de la aplicación de las sanciones previstas en esta LEY. En todo caso, también estas instalaciones estarán sujetas a la regulación y control por parte del Estado".

Artículo 13 mencionado en la ley de especial de Telecomunicaciones Reformada dice que "Es facultad privativa del Estado el aprovechamiento pleno de recursos naturales como el espectro de frecuencias radioeléctricas, y le corresponde administrar, regular y controlar la utilización del espectro radioeléctrico en sistemas de telecomunicaciones en todo el territorio ecuatoriano, de acuerdo a los intereses nacionales."

Mientras el Estado como tal no impida su uso y este no interfiera con sus Frecuencias en lugares de interés nacional no hay problema. Las frecuencias WIFI mencionadas podrán ser utilizadas, pero no cuando interfieran.

Artículo 24 dice lo siguiente: Plan de desarrollo.-(Sustituido inc. 2 por el Art. 7 de la ley 94, R.O. 770, 30-VIII-1995).- El Plan de desarrollo de las Telecomunicaciones capaz de satisfacer las necesidades del desarrollo, para establecer sistemas de comunicaciones eficientes, económicas, y seguras. Las empresas legalmente autorizadas para prestar al servicio público servicio de telecomunicaciones deberán presentar, para aprobación del Consejo Nacional de Telecomunicaciones (CONATEL), un plan de inversiones a ser ejecutado durante el período de exclusividad.

También se debería indagar sobre la legalidad de los servicios de Voz sobre Protocolo de Internet (VoIP). La mayor parte de los países en desarrollo no han decidido todavía si su uso está permitido. En estos países, nada le impide ofrecer los servicios de VoIP.

Sin embargo, en otros países hay una reglamentación complicada sobre VoIP. "En SIRIA está prohibido para todo tipo de redes, no sólo inalámbricas. En UCRANIA, VoIP es legal sólo para llamadas internacionales".

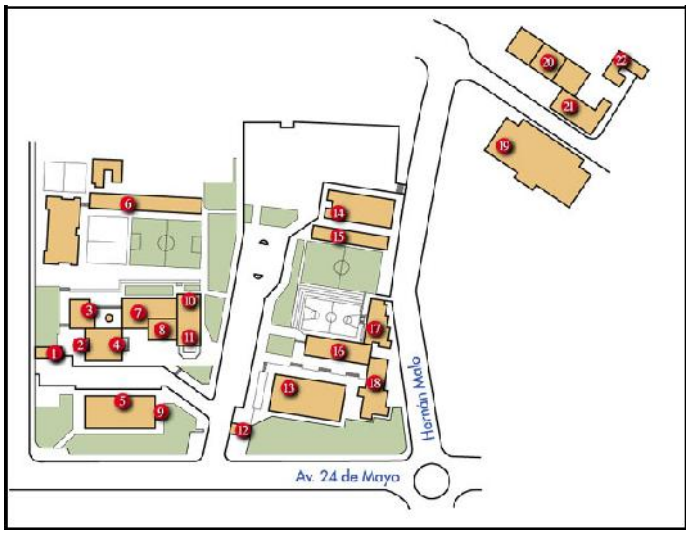
CAPÍTULO 3

ESTUDIO DE POSICIONAMIENTO DE LOS ACCESS POINT PARA DAR UNA MEJOR COBERTURA A LA UNIVERSIDAD DEL AZUAY.

3.1. Distribución Geográfica de los routers de la Facultad de Ciencia y Tecnología.

El Campus principal de la Universidad del Azuay se encuentra localizado en la Ciudad de Cuenca (Av.24 de Mayo 7-77 y Hernán Malo) cuenta con aproximadamente ocho hectáreas de terreno en las que se encuentran 19.557 m2 de construcciones.

Figura 13. Campus Universidad del Azuay.



Fuente: **www.uazuay.edu.ec**

19.Edificio de Ciencia y Tecnología.
Aulas y Laboratorios (Área de Interés).

Aso. Escuela de Ciencia y Tecnología

20. Talleres y Laboratorios [13]
Taller de Mecánica Automotriz

- Aulas y Talleres de Esc. de Electrónica (Área de interés).

Taller de Mecánica Industrial

AIESEC

Sala de Audiovisuales.

Haciendo el previó análisis, estos routers estarían ubicados en la figura 13 de la siguiente página en el Edificio de Ciencia y Tecnología, consta de cuatro pisos, de modo que se colocarían estratégicamente en cada piso como muestra la Figura mencionada.

Se tomó en consideración una red que estipula una capacidad de 500 paquetes, esto está relacionado con la cantidad de computadores que se conectan a la red como un máximo para saturar esa red y debido a que estos a su vez van a estar ocupando un mínimo de 3 aplicaciones nos daría un total de 1500 paquetes que van a ser transmitidos en esta topología de red.

Cada router soporta 256 direcciones IP, por lo tanto sería una configuración de 192.168.1.0 hasta 192.168.1.255 que es su máxima capacidad. También se puede hacer una subred con el siguiente direccionamiento IP 192.168.0.0 hasta 192.168.0.255. lo que nos daría un total de 512 computadores que podrían utilizar la red entre conexiones inalámbricas y computadores.

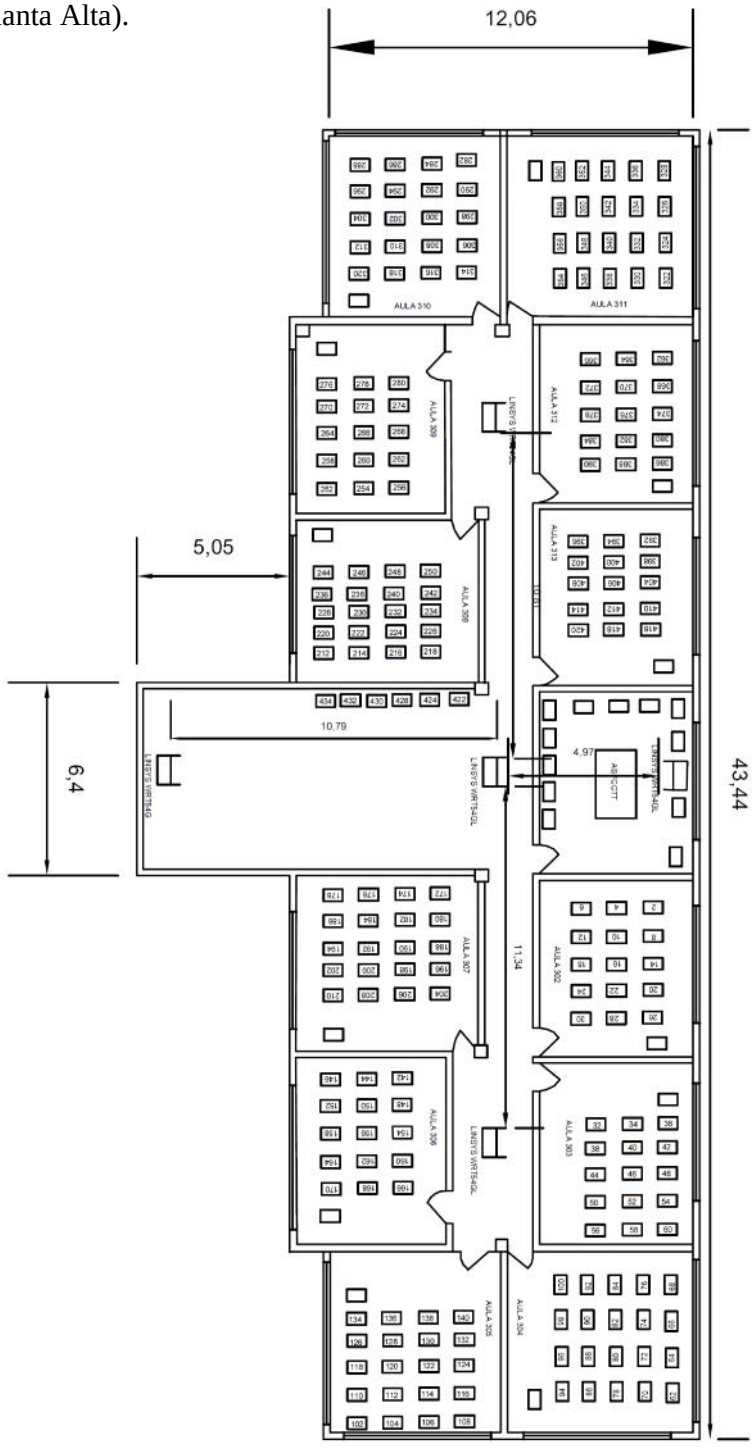
Entonces serían dos routers conectados entre sí por medio de cable estos dos que les he llamado Origen 1 y Origen 2 son los que van hacer la transmisión de la topología MESH; el Origen 1(nodo 1) lo realiza a un solo Router llamado Destino 1 parte del nodo 3 es una topología secuencial en línea recta, el Origen 2(nodo 2) lo realiza a dos Routers llamados: Destino 2 que formarían parte del nodo 4,5 formando una topología en modo Triangulo.

Los routers destinos son tres estos van a distribuir las comunicaciones dentro de su rango de cobertura, a su vez los routers en modo Origen también van a trasmitir dentro de su rango de cobertura para no cruzarse con los otros y evitar el ruido y los efectos de cruce.

Como se puede observar en la Figura 14 se encuentra numerado los asientos que son los puestos de trabajo un total de 422, pero como existen en las demás plantas laboratorios y salas de audio visuales no siempre están ocupados todos lo que permite dar una aproximación de 500 computadores que pueden estar conectados.

3.2. Solución para la colocación de los routers en la Facultad de Ciencia y Tecnología en la U.D.A.

Figura 14. Esquema de colocación de los Routers en la Facultad de Ciencia y Tecnología (Planta Alta).



Fuente: Autor.

3.3. Aproximación de distancias para la colocación de los Routers Inalámbricos.

3.3.1. Planificar Enlaces

Un sistema básico de comunicación comprende dos radios, cada uno con su antena asociada, separados por la trayectoria que se va a cubrir. Para tener una comunicación entre ambos, los radios requieren que la señal proveniente de la antena tenga una potencia por encima de cierto mínimo.

El proceso de determinar si el enlace es viable se denomina cálculo del presupuesto de potencia. El que las señales puedan o no ser enviadas entre los radios dependerá de la calidad del equipamiento que se esté utilizando y de la disminución de la señal debido a la distancia, denominado pérdida en la trayectoria (espacio libre).

3.3.2. Cálculo del presupuesto del enlace

La potencia disponible en un sistema 802.11 puede caracterizarse por los siguientes factores:

Potencia de Transmisión.

Expresada en milivatios, o en dBm. La Potencia de Transmisión tiene un rango de 30 mW a 600 mW, o más. La potencia TX con frecuencia depende de la tasa de transmisión. La potencia TX de un dispositivo dado debe ser especificada en los manuales provistos por el fabricante, pero algunas veces puede ser que no esté disponible. (Flickenger Rob, 2008)

Ganancia de las Antenas.

Las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física. Las antenas tienen las mismas características cuando reciben que cuando transmiten. (Flickenger Rob, 2008)

Por lo tanto una antena de 12 dBi simplemente es una antena de 12 dBi, sin especificar si esto es en el modo de transmisión o de recepción. Las antenas parabólicas tienen una ganancia entre 19 y 32 dBi, las antenas omnidireccionales de 5-17 dBi, y las antenas sectoriales tienen una ganancia de 12-19 dBi.

Mínimo Nivel de Señal Recibida o simplemente, la sensibilidad del receptor.

El RSL (por su sigla en inglés) mínimo es expresado siempre como dBm negativos (-dBm) y es el nivel más bajo de señal que la red inalámbrica puede distinguir.

El RSL mínimo depende de la tasa de transmisión, y la tasa más baja (1 Mbps) tiene la mayor sensibilidad. (Flickenger Rob, 2008)

El mínimo va a ser generalmente en el rango de -75 a -95 dBm. Al igual que la potencia TX, las especificaciones RSL deben ser provistas por elfabricante del equipo.

Pérdidas en los Cables.

Parte de la energía de la señal se pierde en los cables, conectores y otros dispositivos entre los radios y las antenas. La pérdida depende del tipo de cable utilizado y de su longitud. La pérdida de señal para cables coaxiales cortos incluyendo los conectores es bastante baja, del rango de 2-3 dB. Lo mejor es tener cables que sean lo más cortos posibles. (Flickenger Rob, 2008).

Cuando calculamos la pérdida en la trayectoria, se deben considerar varios efectos. Algunos de ellos son pérdida en el espacio libre, atenuación y dispersión. La potencia de la señal se ve disminuida por la dispersión geométrica del frente de onda, conocida comúnmente como pérdida en el espacio libre.

Haciendo a un lado todo lo demás, cuanto más lejanos estén los dos radios, más pequeña la señal recibida debido a la pérdida en el espacio libre. Esto es independiente del medio ambiente, se debe solamente a la distancia. Esta pérdida se da porque la energía de la señal radiada se expande en función de la distancia desde el transmisor.

Utilizando los decibeles para expresar la pérdida y utilizando 2,45 GHz comola frecuencia de la señal, la ecuación para la pérdida en el espacio libre es:

$$L_{fsl} = 40 + 20*\log(r)$$

Donde Lfsl (pérdida de señal en el espacio libre, (Free Space Loss, por su sigla en inglés) es expresada en dB y r es la distancia en metros entre el transmisor y el receptor.

La segunda contribución para la pérdida en el camino está dada por la atenuación. Esto ocurre cuando parte de la potencia de la señal es absorbida al pasar a través de objetos sólidos como árboles, paredes, ventanas y pisos de edificios.

La atenuación puede variar mucho dependiendo de la estructura del objeto que la señal esté atravesando, y por lo tanto es muy difícil de cuantificar.

La forma más conveniente de expresar esta contribución a la pérdida total es agregando una "pérdida permitida" a la del espacio libre. Por ejemplo, la experiencia demuestra que los árboles suman de 10 a 20 dB de pérdida por cada uno que esté en el camino directo, mientras que las paredes contribuyen de 10 a 15 dB dependiendo del tipo de construcción.

A lo largo del trayecto del enlace, la potencia de RF (radio frecuencia) deja la antena transmisora y se dispersa. Una parte de la potencia de RF alcanza a la antena receptora directamente, mientras que otra rebota en la tierra. Parte de esa potencia de RF que rebota alcanza la antena receptora.

Puesto que la señal reflejada tiene un trayecto más largo, llega a la antena receptora más tarde que la señal directa. Este efecto es denominado multitrayectoria, desvanecimiento, o dispersión de la señal. (Rob Flickenger, 2008).

En algunos casos las señales reflejadas se añaden y no causan problemas. Cuando se suman en contra fase, la señal recibida es muy baja llegando inclusive a anularse por las señales reflejadas. Este fenómeno es conocido como **anulación**. Existe una técnica simple utilizada para tratar con la multitrayectoria, llamada diversidad de antena.

Consiste en agregar una segunda antena al radio. De hecho, la multitrayectoria es un fenómeno muy localizado. Si dos señales se suman fuera de fase en una determinada ubicación, no lo harán en otra ubicación en las cercanías.

Si tenemos dos antenas, al menos una de ellas será capaz de recibir una señal utilizable, aún si la otra está recibiendo una señal distorsionada. En aplicaciones comerciales se utiliza diversidad de antenas conmutadas: tienen múltiples antenas en múltiples entradas con un único receptor.

Por lo tanto la señal es recibida por una única antena a un mismo tiempo. Cuandose transmite, el radio utiliza la última antena usada para la recepción.

Los equipos más modernos usan varias cadenas independientes de transmisión, cada una conectada a su propia antena y la correspondiente configuración en el receptor, en lo que se conoce como MIMO (Multiple Input, Multiple Output), lo que consigue mejorar notablemente el caudal neto recibido. Esta es una de las tecnologías utilizadas en el estándar IEEE 802.11n. (Flickenger Rob, 2008)

La distorsión generada por la multitrayectoria degrada la habilidad del receptor de recuperar la señal de manera similar a la pérdida de señal. Una manera simple de tomar en cuenta los efectos de la dispersión para el cálculo de la pérdida en el trayecto es cambiar el exponente del factor distancia en la fórmula de pérdida en el espacio libre.

El exponente tiende a incrementarse con la distancia en un medio ambiente con mucha dispersión. En el exterior con árboles se puede utilizar un exponente de 3, mientras que en el caso de un medio ambiente interno puede usarse uno de 4. (Rob Flickenger, 2008).

Cuando se combinan pérdida en el espacio libre, atenuación y dispersión, la pérdida en el camino es:

L (dB) = 40 + 10*n*log (r) + L (permitida)

Donde **n** es el exponente mencionado.

Para realizar una estimación aproximada de la viabilidad del enlace, se puede considerar solamente la pérdida en el espacio libre. El medio ambiente puede generar pérdida adicional de señal, y debe ser considerado para una evaluación exacta del enlace.
De hecho, el medio ambiente es un factor muy importante, y nunca debe ser descuidado.

Para evaluar si un enlace es viable, debemos conocer las características delos equipos que estamos utilizando y evaluar la pérdida en el trayecto. Cuando hacemos este cálculo, la potencia TX debe ser sumada sólo en uno de los lados del enlace.

Si está utilizando diferentes radios en cada lado del enlace, debe calcular la pérdida para cada dirección (utilizando la potencia TX adecuada para cada cálculo). Sumar todas las ganancias y restar las pérdidas resulta en:

TX Potencia del Radio 1

+ Ganancia de la Antena de Radio 1

- Pérdida en los Cables de Radio 1

+ Ganancia de la Antena de Radio 2

- Pérdida en los Cables de Radio 2

= Ganancia Total

Restar la Pérdida en el trayecto de la Ganancia Total da:

Ganancia Total

- Pérdida en el trayecto

= Nivel de Señal en un lado del enlace

Si el nivel de señal resultante es mayor que el nivel mínimo de señal recibido, entonces "el enlace es viable". La señal recibida es lo suficientemente potente como para que los radios la utilicen. (Flickenger Rob, 2008).

El RSL mínimo se expresa siempre en dBm negativos, por lo tanto -58 dBm es mayor que -72 dBm. En un trayecto dado, la variación en un período de tiempo de la pérdida en el trayecto puede ser grande, por lo que se debe considerar un margen (diferencia entre el nivel de señal recibida y el nivel mínimo de señal recibida).

Este margen es la cantidad de señal por encima de la sensibilidad del radio que debe ser recibida para asegurar un enlace estable y de buena calidad durante malas situaciones climáticas y otras anomalías atmosféricas. (Flickenger Rob, 2008).

Un margen de 10-15 dB está bien. Para brindar algo de espacio para la atenuación y la multitrayectoria en la señal de radio recibida, se debe tener un margen de 20 dB.

Una vez que haya calculado el presupuesto del enlace en una dirección, debe hacer lo mismo en el otro sentido. Substituya la potencia de transmisión delsegundo radio y compare los resultados con el nivel mínimo de señal recibida enel primer radio.

3.3.3. Ejemplo de cálculo del presupuesto del enlace

Como ejemplo, queremos estimar la viabilidad de un enlace de 3 km con un punto de acceso y un cliente. El punto de acceso está conectado a una antena omnidireccional de 10 dBi de ganancia, mientras que el cliente está conectado a una antena sectorial de 14 dBi de ganancia. La potencia de transmisión del AP es 100 mW (ó 20 dBm) y su sensibilidad es -89 dBm. (Flickenger Rob, 2008).

La potencia de transmisión del cliente es de 30 mW (ó 15 dBm) y su sensibilidad es de -82 dBm. Los cables son cortos, con una pérdida de 2 dB a cada lado.

Sumar todas las ganancias y restar todas las pérdidas desde el AP hasta elcliente nos da:

20 dBm (TX Potencia del Radio 1)

+ 10 dBi (Ganancia de la Antena de Radio 1)

- 2 dB (Pérdida en los Cables de Radio 1)

+ 14 dBi (Ganancia de la Antena de Radio 2)

- 2 dB (Pérdida en los Cables de Radio 2)

= 40 dB Ganancia Total

La pérdida en el trayecto de un enlace de 3 km, considerando sólo lapérdida en el espacio libre:

Pérdida en el trayecto = 40 + 20 log (3000) = 109 dB

Restamos la pérdida en el trayecto de la ganancia total:

40 dB - 109 dB = -69 dBm

Ya que -69 dBm es mayor que la sensibilidad del receptor del cliente (-82 dBm), el nivel de señal es justo el suficiente para que el cliente sea capaz de oír al punto de acceso. Solamente hay 13 dB de margen (82 dB–69 dB) que nos permite trabajar bien con buen tiempo, pero habría que analizar si es suficiente para enfrentar condiciones climáticas extremas. (Flickenger Rob, 2008).

Ahora debemos calcular la ganancia desde el cliente hacia el punto de acceso:

15 dBm (TX Potencia del Radio 2)

+ 14 dBi (Ganancia de la Antena de Radio 2)

- 2 dB (Pérdida en los Cables de Radio 2)

+ 10 dBi (Ganancia de la Antena de Radio 1)

- 2 dB (Pérdida en los Cables de Radio 1)

35 dB = Ganancia Total

La pérdida en el camino es la misma en el viaje de vuelta. Por lo tanto nuestro nivel de señal recibido en el punto de acceso es:

35 dB - 109 dB = -74 dBm

Si la sensibilidad de recepción del AP es -89 dBm, nos deja un margen de desvanecimiento de 15 dB (89 dB–78 dB). En general este enlace probablemente va a funcionar pero podría utilizar un poco más de ganancia. Si usamos una antena de 24 dBi en el lado del cliente en lugar de una antena sectorial de 14 dBi, vamos a tener una

ganancia adicional de 10 dBi en ambas direcciones delenlace (la ganancia de la antena es recíproca).

Una opción más cara puede ser la de utilizar radios de más potencia en ambos extremos del enlace, pero debe notarse que si agregamos un amplificador o una tarjeta de más potencia en uno sólo de los extremos, no ayuda a mejorar la calidad global del enlace.

3.4. Análisis de la velocidad de datos.

El **ancho de banda** de una antena se refiere al rango de frecuencias en el cual puede operar de forma correcta. Este ancho de banda es el número de hercios (Hz) para los cuales la antena va a tener una Razón de Onda Estacionaria (SWR) menor que 2:1.

El ancho de banda también puede ser descrito en términos de porcentaje de la frecuencia central de la banda:

$$\text{Ancho de Banda} = 100 \times \frac{FH - FL}{FC}$$

Donde FH es la frecuencia más alta en la banda, FL es la frecuencia más baja, y FC es la frecuencia central. (Flickenger Rob, 2008).

De esta forma, el ancho de banda porcentual es constante respecto a la frecuencia.
Si fuera expresado en unidades absolutas, variaría dependiendo de la frecuencia central.
Los diferentes tipos de antenas tienen variadas limitaciones de ancho de banda.

3.5. Formula de FRIIS aplicada a la simulación.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi}\right)^2$$

P_T =Potencia de Transmisión.
Pr = Potencia de Recepción.
G_T =Ganancia Total.
G_R = Ganancia Receptor.

$D = \left(\frac{1}{\left(\frac{\lambda}{4\pi}\right)^1} \right)^2$.

Asumiendo que es igual a la Distancia se aplica en la fórmula y este valor ya es conocido debido a que es la distancia de cobertura planteada por las mediciones del Plano que realice en la última planta de la Facultad de Ciencia y Tecnología. (Wikipedia, 2014).

$\frac{P_T}{P_t} = G_t G_r (\frac{1}{D^2})$ ^2

De ahí se despeja P_T

$$P_T = \frac{P_r D^4}{G_t G_r (H_r H_T)^2}$$

H_t H_r =1 Este es el valor general de altura en metros del receptor, transmisor; por lo general puede ser la altura que deseamos no infiere mucho en el cálculo por eso se le toma como 1.

Con esta ecuación se basó para sacar los datos de Excel que se verá más adelante para obtener la potencia de trasmisión dado la Potencia de Recepción que contiene el Router, y las Ganancias de Transmisión y Recepción parámetro dado por el Router.

Adicional a eso el Parámetro G_T y G_R son las ganancias que representan a la antena del Router WRT54GL Linksys, este es remplazable eso quiere decir que se puede aumentar, disminuirla ganancia.

3.6. Informes Técnicos.

3.6.1. Tablas para calcular el presupuesto del enlace.

El enrutador Linksys Wrt54GL tiene los siguientes datos de potencia:
Potencia en el Receptor: -65 db para Ofdm 802.11g 54 megs.
-80 db para Dsss 802.11b 11 megs.

Potencia en el Transmisor: 17 dBm. Distancia Transmisor-Receptor 100 m.

Para calcular el **presupuesto** del enlace, simplemente habría que estimar la distancia y completar las siguientes tablas:

Pérdida en el espacio libre a 2,4 GHz

Distancia (m)	100	500	1000	3000	5000	10000
Pérdida (dB)	80	94	100	110	113	120

Tabla 2. Pérdida a través en Decibeles a partir de la Distancia

Pérdidas:

Radio 1 + Pérdida en los cables (dB)	Radio 2 + Pérdida en los cables (dB)	Pérdida en el espacio libre (dB)	= Pérdida Total (dB)
17 -3dB	17 – 0dB	-80dB	-83dB.

Presupuesto para el enlace de Radio 1 a Radio 2:

Potencia TX de Radio 1	+ Ganancia de la Antena	- Pérdida Total	= Señal	>Sensibilidad del Radio 2
17dBm	2dB	-83dB	-64dB	-64dBm

Supongamos que el Radio 2 es el que hace la función de repetir la señal a los usuarios finales que pueden ser los computadores ya sea inalámbricos o con estructura cableada, la cobertura de red se fija solo a una área determinada, por tanto su transmisión contiene menos pérdida. Presupuesto para el enlace del Radio 2 a Radio 1:

Potencia TX de Radio 2	+ Ganancia de la Antena	- Pérdida Total	= Señal	>Sensibilidad del Radio 1
17dBm	2dB	-80dB	-61dB	-61dBm

Habría que analizar si la señal recibida esta con interferencia.

Si la señal recibida en el radio 2 es mayor que la intensidad mínima de señal recibida enel radio 1 en ambas direcciones del enlace, entonces el enlace es viable.

Con las justas llega a estar en el margen permitido que es 3 dBm, de diferencia entre los dos enlaces de sensibilidad de radio.

CAPÍTULO 4

CONFIGURACIÓN DEL ENRUTADOR MESH.

4.1. Procedimientos para la configuración y simulación de la Red Ad-Hoc.

El sistema operativo GNU/Linux brinda al administrador de red acceso completo a muchos elementos del trabajo en redes. Podemos acceder y manipular paquetes de red a cualquier nivel, desde la capa de enlace de datos,hasta la capa de aplicación.

Se pueden tomar decisiones de enrutamiento con base en cualquier información contenida en el paquete de red, desde la dirección de enrutamiento y puertos, hasta los contenidos de los segmentos de datos. (Flickenger Rob, 2008).

Un punto de acceso basado en Linux puede actuar como enrutador, puente, corta fuego, concentrador VPN, servidor de aplicaciones, monitor de la red, o virtualmente cualquier otro desempeño de la red en el que se pueda pensar.

Es un software libre, y no requiere pagos de licenciamiento. GNU/Linux es una herramienta muy poderosa que puede acoplarse a una amplia variedad de desempeños en una infraestructura de red. (Flickenger Rob, 2008).

Agregar una tarjeta inalámbrica y un dispositivo Ethernet a una PC queejecuta Linux dará una herramienta muy flexible que puede ayudar a repartir el ancho de banda y administrar su red a un costo muy bajo.

El equipamiento puede ser desde una computadora portátil reciclada, o una computadorade escritorio, hasta una computadora, tales como un equipo de red Linksys WRT54GL, o Buffalo.

En esta sección veremos los procedimientos para la configuración y simulación de una red ad-hoc en Linux:

- Crear una red ad-hoc real basada en tecnología IEEE 802.11bg.El puente puede usarse tanto como un simple punto de acceso, o como un repetidor con dos radios.

4.1.1. Prerrequisitos

Antes de comenzar, hay que estar familiarizado con Linux desde la perspectiva del usuario, y ser capaz de instalar la distribución GNU/Linux de nuestra elección. También se requiere de una comprensión básica de la interfaz de línea de comando (Terminal) en Linux. (Flickenger Rob, 2008).

Se necesita por lo menos tres computadoras con una o más tarjetas inalámbricas instaladas previamente, así como una interfaz Ethernet estándar. Estos ejemplos utilizan una tarjeta y un manejador (driver) específicos, pero hay varios tipos diferentes de tarjetas que pueden funcionar bien. (Flickenger Rob, 2008).

Las tarjetas inalámbricas basadas en los grupos de chips Atheros y Prism lo hacen particularmente bien. Estos ejemplos se basan en la versión de Linux Ubuntu, con una tarjeta inalámbrica compatible con los manejadores HostAP o MADWiFi.

Para completar estas instalaciones se requiere del siguiente software, el cual debe estar incluido en su distribución Linux:

• Herramientas Inalámbricas (comandos iwconfig, ifconfig)

• Cortafuego IPTables

• Dnsmasq (servidor caché DNS y servidor DHCP)

La potencia de CPU que se requiere depende de cuánto trabajo se tiene que hacer por encima de un simple enrutamiento y NAT. Para muchas aplicaciones una computadora de capacidad tan mínima como: 486, o de 133 MHz es perfectamente capaz de enrutar paquetes a las velocidades inalámbricas.

Un enrutador típico que solo esté realizando NAT puede operar con tan solo 64 MB de RAM y almacenamiento (Perpinan Antonio, 2002).

En consecuencia se puede utilizar almacenamiento de estado sólido, como un disco flash, en lugar de un disco duro, proveerá más eficiencia.

4.1.2. Escenario 1: Puntode acceso en modo Ad-Hoc.

Configuración Inicial

Para comenzar con una computadora ya configurada para ejecutar GNU/Linux.Podemos optar con la instalación de Ubuntu Servidor, o Fedora Core.En mi caso escogí Ubuntu Servidor. Para su funcionamiento, la computadora debe tener al menos dos interfaces, y al menos una de ellas debe ser inalámbrica. El resto de esta descripción supone que su puerto Ethernet (eth0) está conectado a la Internet, y que hay una interfaz inalámbrica (wlan0) que va a proveer la funcionalidad del punto de acceso.

Para saber si el grupo de chips admite el modo maestro, se prueba con el siguiente comando en modo raíz (root):

iwconfig wlan0 mode Master

Lo típico es recibir un error cuando tecleamos esta instrucción y se debe a que nuestra tarjeta inalámbrica no es compatible con este modo, por lo que se debe cambiar de instrucción a:

iwconfig wlan0 mode Ad-hoc.

Como podremos ver en el Anexo, el error existe todavía lo cual nos imposibilita a cambiar de modo para lograr nuestro objetivo.
Se procede a operar de distinta forma:
Primero apagamos la tarjeta de red inalámbrica de la interfaz wlan0:
ifconfig wlanX down
x representa la tarjeta que tenemos instalada en mi caso es “cero”(0)
Si tenemos más tarjetas inalámbricas, dependiendo del driver la interfaz cambiará a wlan 1, 2, etc.
Enseguida de haber puesto ese comando ponemos lo que sigue, lo que era nuestro objetivo.
iwconfig wlan 0 mode Ad-hoc.

Cuando damos enter, el resultado es una pantalla vacía, significa que nuestro modo Ad-hoc es reconocido por la tarjeta inalámbrica.

Últimamente procedemos a levantar el interfaz inalámbrico con el siguiente comando:

ifconfig wlanX up

Damos enter después de haber escrito el comando, y el resultado es que nuestra interfaz inalámbrica cambio a modo ad-hoc.

Estos tres pasos lógicos se deben hacerlo lo más pronto posible, ya que el driver que maneja la tarjeta inalámbrica comenzará a buscar nuevas redes inalámbricas y se conectará enseguida a otra red inalámbrica, lo cual nos hará fallar.

El siguiente paso es asignar el nombre del dispositivo de red, por ejemplo: Esteban.

sudo iwconfig wlan0 essid “Esteban”

Presionamos enter y ya tenemos el nombre de la conexión de red.

Ahora asignamos a la tarjeta de red la dirección IP para establecer la transmisión con el siguiente comando:

sudo ifconfig wlanX <dir_ip

Una vez hecho esto nuestra trasmisión quedará establecida, y lo más interesante es que se genera automáticamente un terminal de transmisión que podemos comprobar si se estableció la dirección IP con el siguiente comando.

ifconfig

Nos muestra los adaptadores de red lo, wlan0, eth0 (interfaz que utiliza el puerto Ethernet). Y con esto comprobamos que la dirección se estableció con éxito.

Procedemos ahora hacer ping, con los otros usuarios que deseamos hacer la red ad-hoc que serían tres usuarios (computadores) por lo mínimo, puede ser cualquier dirección de red.

ping 192.168.0.101. Computadora 1.

ping 192.168.0.102. Computadora 2.

ping 192.168.0.103. Computadora 3.

Ahora se procede hacer ping entre computadoras: ping 1-3; 3-1; 2-3; 3-2; 2-1;1-2.

Y esto despliega una cantidad de resultados en pantalla con tiempos de respuesta entre computadores.

Al hacer ping, logramos que se establezca la comunicación entre computadores inalámbricos.

Se debe repetir estos procedimientos de configuración en los tres computadores
Los resultados de esta conexión se ilustrarán en el Anexo.

Reemplazando WLAN0 con el nombre de su interfaz.

De todas formas se puede probar con la misma configuración en el modo ad hoc, o Managed que es permitido por todos los grupos de chips. Esto requiere configurar todas las computadoras portátiles que están conectadas al "punto de acceso" en el modo Ad hoc, y puede que no funcione del modo que seestaba esperando. (Perpinan Antonio, 2002).

En general es mejor encontrar una tarjeta inalámbrica que admita el modo AP. Antes de continuar asegurarse de que dnsmasq está instalado en su computadora. Puede utilizar laherramienta de configuración gráfica de su distribución para instalarlo.

En Ubuntu puede simplemente correr lo siguiente enmodo raíz:

apt-get install dnsmasq.

4.1.3. Configurar enmascarado en el kernel Escenario 2: Hacer del punto de acceso un puente transparente.

Este escenario puede utilizarse tanto para un repetidor de dos radios, o para un punto de acceso conectado a una Ethernet. Utilizamos un puente en lugar de un enrutador cuando queremos que ambas interfaces en el punto de acceso compartan la misma subred.

Esto puede ser particularmente útil en redes con múltiples puntos de acceso donde preferimos tener un único cortafuego central y tal vez un servidor de autentificación. Dado que todos los clientes comparten la misma subred, pueden ser manejados fácilmente con un único servidor DHCP y un cortafuego sin la necesidad de un relevador DHCP.

Por ejemplo, se puede configurar un servidor como en el primer escenario, pero utiliza dos interfaces Ethernet cableadas, en lugar de una cableada y una inalámbrica. Una interfaz sería su conexión a Internet, y la otra conecta a un conmutador. Luego se conecta tantos puntos de acceso como se necesite, al mismo conmutador,

Configurándolos como puentes transparentes, y cada uno pasará através del mismo cortafuego y utilizará el mismo servidor DHCP.

La simplicidad de "puentear" tiene un costo en cuanto a eficiencia. Ya que todos los clientes comparten la misma subred, el tráfico de difusión se repite a través de la red. Esto funciona bien con redes pequeñas, pero cuando el número de clientes se incrementa, se desperdicia mucho ancho de banda en el tráfico, y se vuelve complejo establecer rutas entre los nodos (computadores). (Perpinan Antonio, 2002)

Configuración Inicial

La configuración inicial para un punto de acceso puenteado es similar al del punto de acceso enmascarado, sin requerir de dnsmasq. Se sigue las instrucciones de configuración inicial del ejemplo anterior. (Perpinan Antonio, 2002).

Además, para la función de puente se requiere el paquete bridge-utils. Este paquete está disponible para Ubuntu y otras distribuciones basadas en Debian. Asegurarse de que éste esté instalado y de que el comando brctl esté disponible antes del procedimiento.

Configurando las Interfaces

En Ubuntu o en Debian configuramos las interfaces editando el archivo **/etc/**

network/interfaces.

Agregar una sección como la que sigue, pero cambiar los nombres de las interfaces y las direcciones IP que correspondan. La dirección IP y la máscara de red deben concordar con la de su red. Este ejemplo supone que está construyendo un repetidor inalámbrico con dos interfaces inalámbricas, wlan0 y wlan1. La interfaz wlan 0 va a ser un cliente de la red "oficina", y wlan1 va a crear una red llamada "Repetidor".

Se agrega lo siguiente a **/etc/network/interfaces**:

Para configurar las interfaces se utiliza el comando Nano.

Ej: Nano /etc/network/interfaces, y se procede a escribir lo siguiente:

auto br0 # Suponemos que esta interfaz es del Access point principal que lleva conectado el cable de red, obviamente es de otra marca madwifi (controlador), o Prism, pero no de atheros.

iface br0 inet static # Estamos poniendo una dirección de red estática.

address 192.168.1.2

network 192.168.1.0

netmask 255.255.255.0

broadcast 192.168.1.255

gateway 192.168.1.1 # Dirección del que está dando el internet o compartiendo las subredes.

pre-up ifconfig wlan0 192.168.0.101 up # configurando la interfaz wlan0 y wlan1.

pre-up ifconfig wlan1 192.169.0.102 up

pre-up iwconfig wlan 0 essid “Oficina” mode Managed #Tenemos dos interfaces inalámbricas wlan 0, y wlan 1; la una está en modo Administrador, y la otra en modo Repetidor de la señal.

pre-up iwconfig wlan1 essid “Repetidor” mode Ad-Hoc

bridge_ports wlan0 wlan1 # Estableciendo el Puente entre wlan0 y wlan1

post-down ifconfig wlan1 down

post-down ifconfig wlan0 down

Poner una marca de comentario con numeral a todas las líneas que se refieran a wlan 0, o a wlan 1 para asegurarse de que no van a interferir con nuestra configuración. Esta sintaxis para configurar los puentes mediante el archivo **interfaces** es específica para distribuciones basadas en Debian, y los detalles de la configuración del puente son manejados por un par de guiones: /**etc/network/ifpre-up.d/bridge** y **/etc/network/if- post-down.d/bridge**. La documentación para estos guiones se encuentra en **/usr/share/doc/bridge-utils/**

Arrancar el Puente

Una vez que el puente esté definido como una interfaz, se arranca el puente escribiendo:

ifup -v br0

La "-v" significa salida verbosa y proporciona información acerca de lo que está pasando.

4.1.4. Configuración del Router Linksys WRT54GL.

Instalación

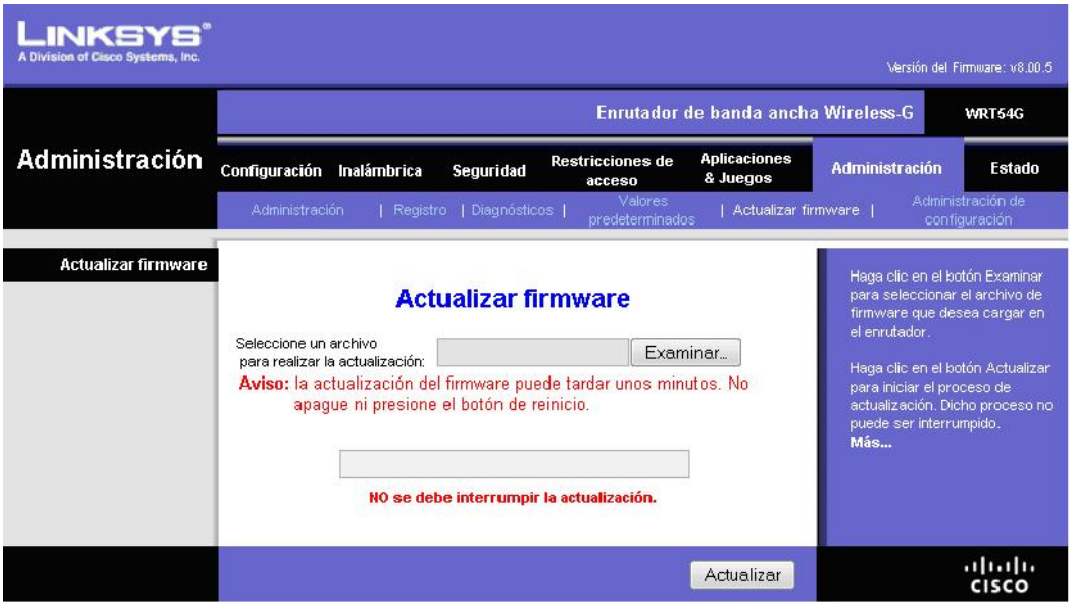
La instalación de un firmware puede realizarse a través de la interfaz Web o por TFTP (Trivial File Transfer Protocol), la primera de ellas no es soportada por todos los firmware, además la interfaz Web debe guardarse en memoria y si este recurso es limitado en el enrutador, por otro lado es mucho más sencillo hacer cambios a través de la Interfaz Web. (Linksys, 2014).

Finalmente es necesario saber instalar el firmware a través de TFTP ya que si el firmware está dañado es la única forma de hacerlo.

- Instalación por interfaz Web: Es la manera más sencilla de realizar la instalación del firmware, simplemente se busca en la interfaz una pestaña que indique actualización de firmware o en ingles firmware upgrade después se debe dar la dirección donde se encuentra el código, a continuación se presenta una imagen de este procedimiento usando el firmware que viene de fábrica en la Figura 15. (Linksys, 2014).

.

Figura 15. Página de Configuración del Enrutador



Fuente: Autor.

Proceso de arranque: Cuando el linksys arranca el PMON (versiones 1 y 1.1) ó CFE que son cargadores de arranque toman el control del proceso de arranque, esta revisa si existen particiones en la NVRAM (Memoria no volátil de acceso aleatorio) si no existen entonces las realiza usando los valores almacenados en el cargador de arranque, después revisa el parámetro boot_wait si este parámetro esta encendido es decir está en *on*, el espera conexiones de un servidor TFTP por un tiempo predeterminado que comúnmente es de tres segundos, a continuación realiza un chequeo de redundancia cíclica sobre el firmware, si es correcto el arranque se ejecuta normalmente, de lo contrario el cargador de arranque esperara hasta que un nuevo firmware se reciba vía TFTP. (Linksys, 2014).

Cuando sucede esto en el enrutador hace varias cosas que vale la pena mencionar, crea algunas IP con las que hace cosas como responder solicitudes ARP para la dirección 192.168.1.1, escuchar mensajes ARP de difusión y responder a la solicitud ICMP de ping. Por otra parte cuando se inicia el modo de *boot_wait* el inicia TFTP sin necesidad de contraseña.

Una ventaja de los cargadores de arranque es que difícilmente se dañan porque no se permite escritura en la partición de la NVRAM en que se encuentra este.

Instalación del firmware por TFTP: Para instalar el firmware vía TFTP se aprovecha el boot_wait que es el estado en el que el enrutador esperara una conexión de servidor TFTP, sin embargo no siempre está habilitada esta opción así que se pueden usar tres técnicas para activarlas según la versión y los conocimientos del usuario: Ping Hack, a través de líneas de comando del sistema operativo ó como última opción actuando directamente sobre el cargador de arranque a través de puerto serial. (Linksys, 2014).

Existen diferentes comandos para TFTP y depende del sistema operativo que se utilice, esto se debe tomar en cuenta siempre que se quieran hacer modificaciones a través de esta vía.

Versiones de los Firmware

Firmware Original

Basado en Linux sirvió como base para crear otros, no es hackeable, soporta WPA-PSK y WPA2-PSK, solo algunas versiones soportan WPA (Wi-FI protected access) y WEP (wireless encryptation protocol).

Este firmware es adecuado para usuarios promedio que simplemente quieren que su enrutador funcione de inmediato y no están interesados en hacer modificaciones.

Instalación OpenWrt

La manera más fácil de instalar el firmware es desde la interfaz web original, en Administración / actualizar firmware y pulsar sobre el botón examinar se despliega la ventana que permite buscar el archivo .bin que contiene el instalador del firmware.

La versión de firmware a instalar es la 8.09.2 para el kernel 2.4 que se encuentra en la sección de descargas del portal web www.openwrt.org de la comunidad OpenWrt quienes desarrollaron el firmware. El proceso de instalación dura algunos minutos y durante este tiempo no se debe apagar el dispositivo. (OpenWrt, 2013).

CONFIGURACIÓN DE LAS INTERFACES.

Inicio.

Después de la correcta instalación del firmware se accede por medio de un explorador de internet al portal de inicio de OpenWrt que se muestra en la Figura 16 que generalmente se encuentra en la dirección 192.168.1.1, para poder modificar los parámetros predefinidos en el firmware se debe acceder a la pestaña de administración que se encuentra en la parte superior derecha. Esta solicita el usuario y la contraseña que por defecto es root y admin respectivamente.

Figura 16. Portal OpenWrt.

Fuente: Autor

Aunque la interfaz gráfica facilita las modificaciones en la configuración es necesario implementar comandos en la consola del router por medio de protocolos como Telnet y SSH. Por defecto el puerto habilitado para acceder a consola es el de Telnet mientras que el puerto SSH no está habilitado.

Para mayor seguridad se deben utilizar sesiones SSH en lugar de Telnet, es necesario cambiar la contraseña por defecto para habilitar el puerto para SSH, esto a su vez deshabilita el puerto de Telnet.

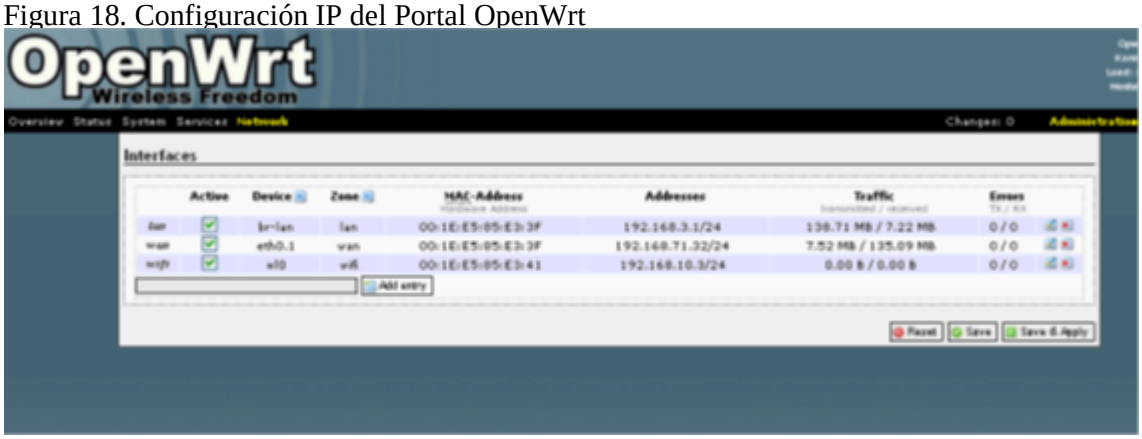
En la Figura 17 se puede ver el cambio de contraseña se realiza después de presionar Administration, vamos a la pestaña System y finalmente Admin Password tal como se presenta a continuación.

Figura 17. Configuración del Portal OpenWrt.

Fuente: Autor

Primero se revisa que interfaces están creadas en enrutador, para lo que se accede a la pestaña Network/Interface, aquí deben estar WAN, LAN y Wi-FI, si alguna de estas falta se debe crear usando el botón Add entry, es importante escoger el dispositivo (Device) adecuado tal como se presenta en la Figura 18. (OpenWrt, 2013).

Figura 18. Configuración IP del Portal OpenWrt



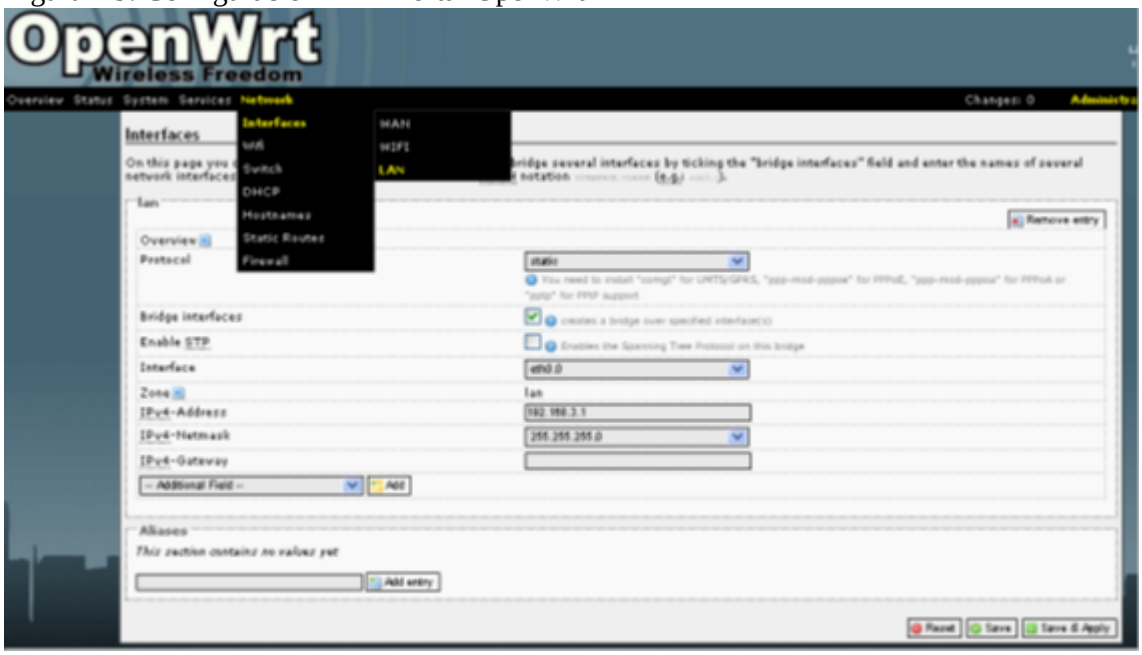
Fuente: Autor.

Otro paso importante es colocar una dirección IP de manera lógica con la arquitectura de red, para la red LAN se utilizó la siguiente lógica para asignar IP, la dirección de la interfaz cableada es 192.168.x.1 donde la x corresponde al número del nodo y para la interfaz inalámbrica 192.168.10.x, esta modificación se realiza fácilmente en la interfaz gráfica.

LAN.

En la Figura 19 se encuentra la configuración LAN para la red cableada se dirige a la pestaña Network/Interfaces/LAN tal como se muestra a continuación, el ejemplo se realiza con el nodo 3. (Linksys, 2014).

Figura 19. Configuración LAN Portal OpenWrt

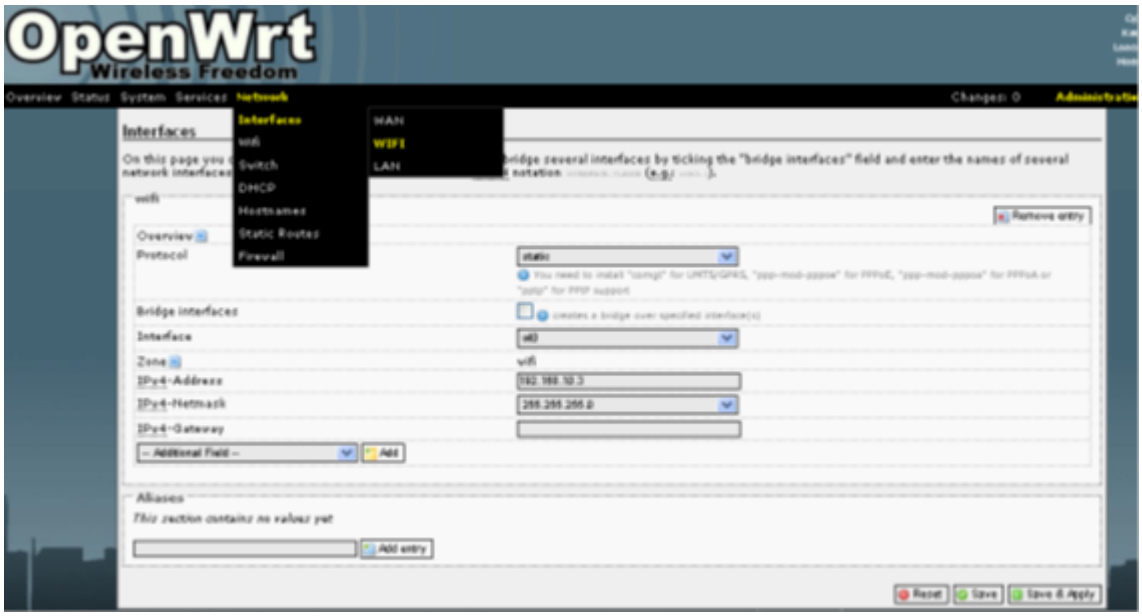


Fuente: Autor.

INALÁMBRICA

En la Figura 20 se encuentra la interfaz inalámbrica se configuran los campos como se presenta ahora, accediendo a las modificaciones por Network/Interfaces/Wi-FI. (Linksys, 2014).

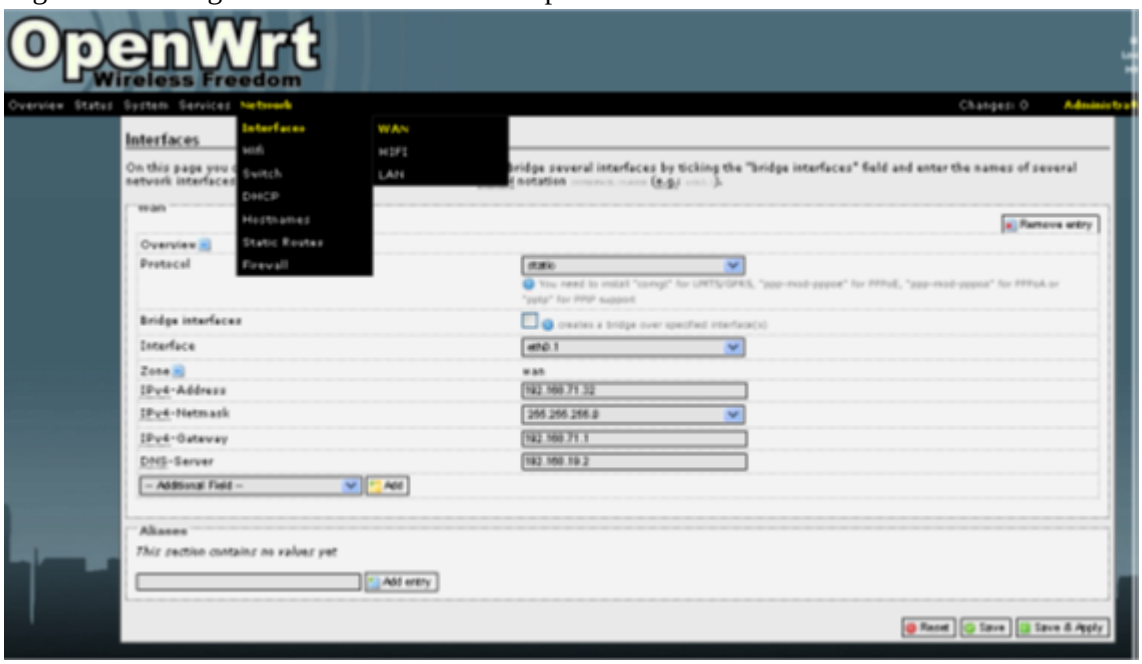
Figura 20. Configuración Inalámbrica del Portal OpenWrt.



WAN

En la Figura 21 está listo para configurar el puerto WAN que es el encargado de recibir la conexión a Internet, se accede a la pestaña Network/Interfaces/WAN y se habilita para que trabaje con DHCP si está disponible, sino se llenan los campos de dirección IP, mascara de subred, puerta de enlace y servidor DNS de acuerdo con nuestro ISP.

Figura 21. Configuración WAN del Portal OpenWrt



Fuente: Autor

Instalación Paquetes

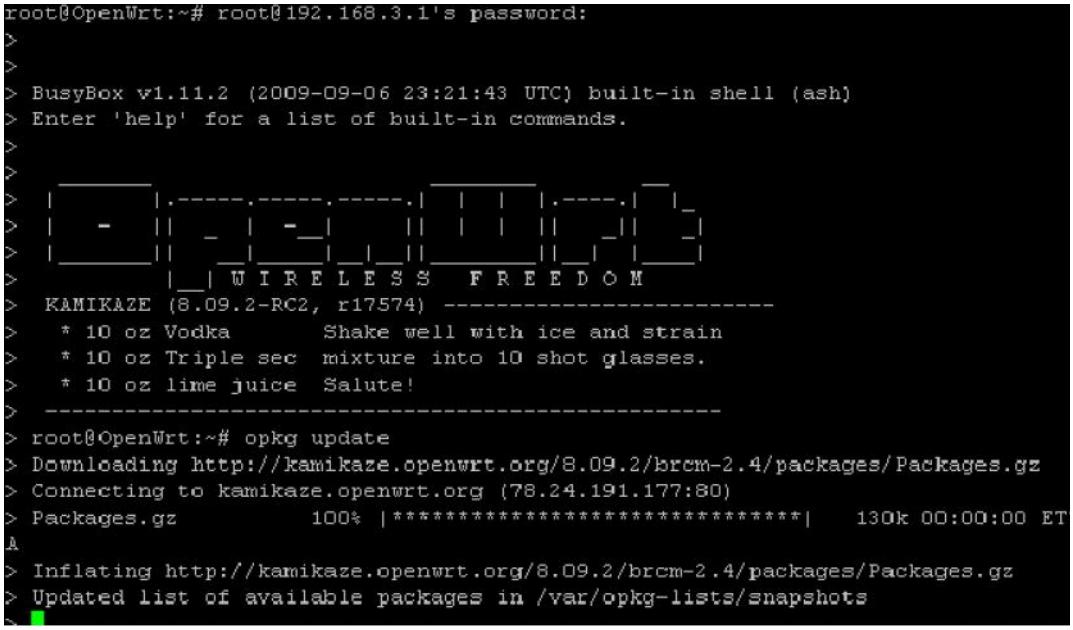
Repitiendo todo el proceso anterior con cada nodo se establece la red inalámbrica ad-hoc, pero sin protocolo de enrutamiento, lo cual implica que no tendrá la suficiente información en la tabla de rutas necesaria para acceder a otros nodos que estén fuera del área de cobertura de la interfaz inalámbrica, y a las interfaces LAN de cada nodo MESH. Para lo anterior es necesaria la instalación de diversos paquetes correspondientes a los protocolos de enrutamiento a implementar los cuales se encuentran en los repositorios de OpenWrt a través de una sesión SSH a la dirección 192.168.3.1 (en este caso el 3) accediendo a la terminal de comandos del enrutador y en donde con el comando Opkg es el encargado de la gestión de paquetes del firmware. Su sintaxis se presenta en la siguiente Tabla 3:

Tabla 3. Tabla de Comandos del OpenWrt

Comando	Función
Opkg update	Descarga la lista de paquetes disponibles en los servidores de los repositorios
Opkg install nombre_paquete	Descarga el paquete seleccionado del repositorio y lo instala.
Opkg remove Nombre_paquete	Desinstala o remueve el paquete seleccionado.

Fuente: OpenWrt

Figura 22. Instalación de Paquetes de OpenWrt.



Fuente: Autor

En la Figura 22 se encuentra la instalación de Paquetes de OpenWrt y se muestra como se están instalando los Paquetes de la dirección URL:

http://Kamidaze.openwrt.org/8.09/brcm-2.4/packages/Packages.gz

Como se puede ver está instalado al 100% y este ya se encuentra instalado en el computador que es el que contiene el Firmware.

Impedimentos para implementar RIP en Redes inalámbricas Ad-Hoc

Configuradas correctamente las interfaces del enrutador Linksys es necesario implementar un protocolo de enrutamiento sobre la interfaz inalámbrica de cada enrutador la cual está configurada en modo ad-hoc.

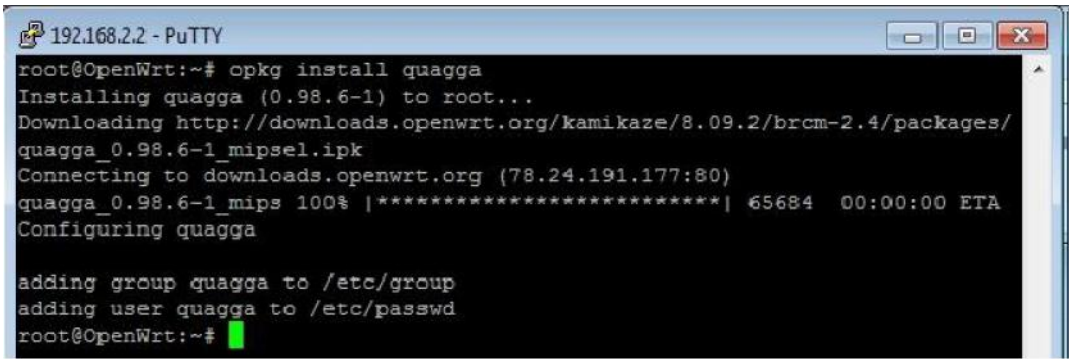
Al inicio del trabajo de investigación se estudiaron los protocolos de enrutamiento y sus categorías más importantes de acuerdo al algoritmo usado para determinar las rutas, los cuales son Vector distancia, tomándose como punto de partida los protocolos RIP como referencias principales.

Para la implementación de los protocolos RIP en el enrutador es necesaria la instalación del paquete Quagga que se encuentra en los repositorios del OpenWrt.

Quagga es una recopilación de software de enrutamiento que provee a sistemas de la familia Unix entre los cuales se encuentra FreeBSD, Solaris, NetBSD, Linux y por consiguiente para el firmware OpenWrt.

Quagga es una bifurcación del proyecto GNU Zebra el cual fue lanzado como parte del proyecto GNU y este demonio que se encarga de manejar las tablas de rutas del núcleo. Quagga soporta los protocolos OSPFv2, OSPFv3, RIP v1 y v2, RIPng y BGP-4. Se puede realizar la instalación por medio del comando: Opkg install quagga como se observa a continuación en la Figura 23.

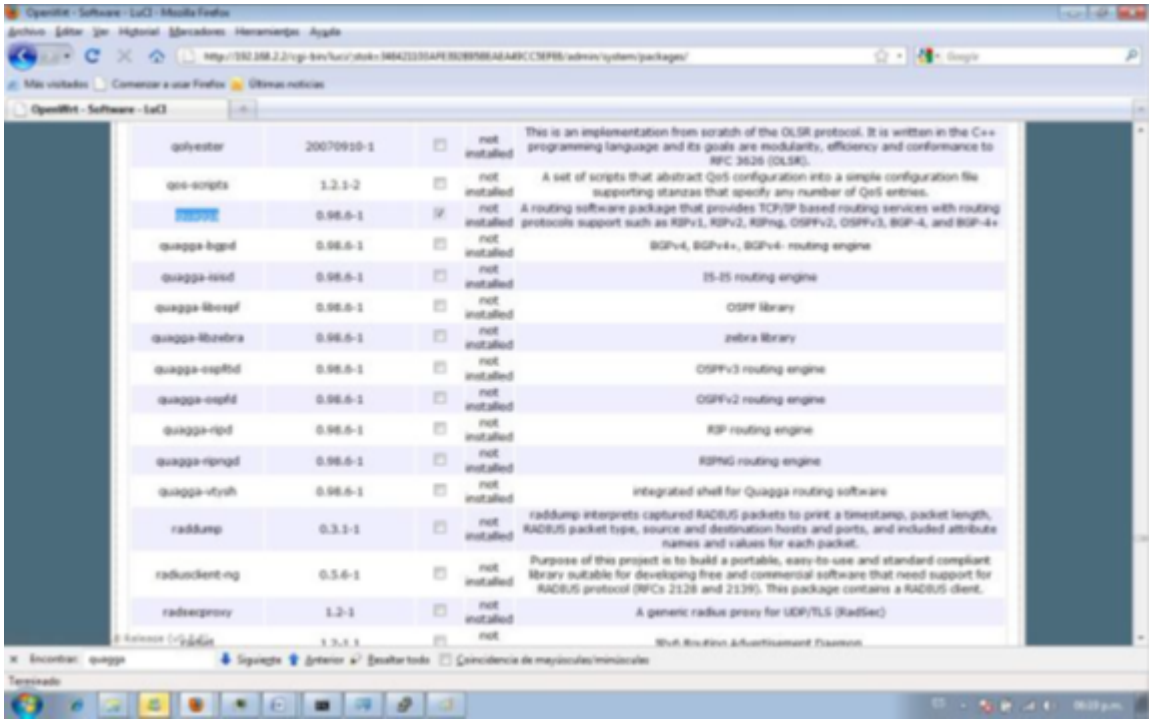
Figura 23. Terminal SSH por medio de PuTTY.



Fuente: Autor

Por medio de la interfaz Web del firmware que se muestra en la Figura 24 se denota que quagga es necesario seleccionar los paquetes correspondientes a los protocolos a ejecutar por el software quagga.

Figura 24. Interfaz WEB para la configuración de los Paquetes de OpenWrt.



Fuente: Autor.

El impedimento se da ya que los desarrolladores de quagga hicieron sus software's para redes de topología cableada y no le pusieron mucho énfasis en redes más grandes como en la inalámbrica, lo mucho que se puede hacer es la transmisión de dos enrutadores conectados a la vez en forma inalámbrica, el uno que se mantiene en modo infraestructura, y los otros dos en modo ad-hoc para transmitirse entre ellos, pero el momento que aparece otro nodo más o enrutador ya no está diseñado para que lo reconozca, la solución sería poner a dos enrutadores en modo infraestructura y trasmitir dos enrutadores inalámbricos con el uno y con el segundo en modo infraestructura transmitir un enrutador más no dos para completar mi implementación propuesta de cinco puntos de acceso o enrutadores ya que esto sí es posible realizar.

CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES

- Una red MESH es una red descentralizada, puede tener administrador de la red o carecer de este.
- El término MESH hace referencia a las redes móviles de capacidad ad hoc.
- Los elementos que un usuario necesita para crear una red MESH son únicamente puntos de acceso (dispositivos de red wireless) funcionando en modo ad-hoc y al menos uno haciéndolo también en modo infraestructura para proporcionar acceso a Internet a todos los usuarios de la red.
- OpenWrt es un software de distribución de Linux libre para sistemas empotrados y es de característica configurable.
- La mejor implementación que se adapta a las necesidades de una red de topología MESH es D.S.D.V. Destino Secuencial Vector Distancia, dicho protocolo nos sirvió para ejemplificar la topología de red de la forma más adaptable.
- El proceso de determinar si el enlace es viable se denomina cálculo del presupuesto depotencia.
- Para tener una visión clara es necesario hacer el cálculo del presupuesto del enlace.
- Medir potencias, en trasmisor y receptor.
- Hay dos tipos de escenarios, el uno punto de acceso en modo ad-hoc, el segundo es hacer del punto de acceso un puente transparente.
- Una forma fácil es aprovechar las distribuciones de Linux y hacer arrancar desde un cd el software de configuración de la red MESH, pero no era el objetivo del estudio.

- Un punto de acceso basado en Linux puede actuar como enrutador, puente, corta fuego, concentrador VPN, servidor de aplicaciones, monitor de la red, o virtualmente cualquier otro rol de la red en el que se pueda pensar.
- Para poder utilizar las distribuciones Linux hay que tomar en cuenta que cada router debe ser flasheado (Instalado en la memoria interna RAM), para poder obtener esta topología de red.
- La mejor topología de red que se puede ejemplificar es la DSDV, debido a que no fue creado para una red metropolitana, porque no se presta para eso en sus configuraciones, en cambio los otros protocolos fueron creados para redes grandes, en donde muchos usuarios se pueden conectar a la vez sin saturar la carga del servidor CPU.
- Cuando se habla de un modelo de redes inalámbricas sea sostenible se estimará un tiempo de 5 años, o más.
- No hay como hacer un mismo diseño de redes inalámbricas que se aplique a todas partes, se necesita hacer un estudio minucioso del lugar, con todas sus características geográficas, climáticas, etc, que no siempre son las mismas.
- Para transmitir con mayor Throughput se concluyó que se debe transmitir en norma G, para menores transmisiones con norma B, estos resultados fueron apreciados en la simulación de la red en los Anexos.
- La capacidad que debe tener un Router en su cantidad de usuarios es 256 usuarios.
- La capacidad que debe tener una red Inalámbrica en Megabytes/seg es de 55 Megabytes/Seg.
- La capacidad que debe tener una red Alámbrica en Megabytes/seg es de 100 Megabytes/Seg.

RECOMENDACIONES

- No hay como esperanzarse en Roofnet como una solución económicamente viable, ya que este protocolo proactivo fue adoptado por el Meraki, compañía de E.E.U.U, y ellos se apoderaron de su licencia, lo cual no es ilegal, mientras que no se actualicen su software gratuito por motivos de costo de la nueva licencia, y no dejan utilizar este en enrutadores de terceros.
- No hay como elegir un solo modelo de redes inalámbricas que sea sostenible.
- Para poder calcular aproximaciones de distancias se deberá analizar los obstáculos pertinentes, entre radio enlaces, formulándose unas tablas con datos y analizando por medio de la siguiente pregunta ¿hasta cuándo se puede obtener señal sin que esta se desvié, o se pierda?
- Para poder hacer un análisis de costos habría que darse cuenta bien de los análisis técnicos, y de la sostenibilidad económica.
- Puede ser peligroso escribir en una memoria Flash de un router, ya que si lo hacemos mal, podemos perder las características esenciales de este, habrá que analizar si el router es de capacidad compatible y si hay soporte al software de distribución.
- En el Router Linksys hay una opción en la interface del OpenWrt, tipo de trasmisión, escoger la opción mixed. Esta opción hace que seleccione automáticamente, norma G o B, según la cantidad de información que es consumida por todos los usuarios de dicha red.
- Debido a que en la Facultad de Ciencia y Tecnología (Edificio), el Backbone (Instalaciones de Fibra Óptica) soportan hasta 10 Gb, se aconseja para poder utilizar la red MESH junto con los Routers, adquirir un conversor de Fibra a Ethernet, puede ser mono modo, o multi modo.
- Para poder utilizar más usuarios en la red propuesta se debe conectar en modo Cascada los routers para sacarle el mayor provecho a la cantidad de usuarios.

BIBLIOGRAFÍA

Referencias Bibliográficas

REID Neil. 2004. Manual de Redes Inalámbricas. Edición 1. Pág. 104. ISBN: 970104147X.

FLICKENGER Rob. 2003.Building Wireless Community Networks, 2nd Edition. 186p. ISBN: 978-0-596-00502.3.

FLICKENGER Rob. 2008. Redes Inalámbricas en los Países de Desarrollo. Tercera Edición. 413p. ISBN: 978-0-9778093-7-0.

PERPINAN Antonio. 2002. Administración de redes GNU/LINUX. 450 Pág. ISBN: 88-99999-99-9.

IBAÑEZ Guillermo. 2006. Wi-Fi: Aspectos técnicos, seguridad y redes Mesh. 123 Pág. ISBN: 84-89416-44-3.

CELADOR Goméz. 2006. Wireless. Los Mejores Trucos. 2da Edición. 480 Pág. ISBN: 8441519978.

CABEZAS Granado Luis Miguel, **GONZÁLES** Lozano Francisco José. 2010. Redes Inámbricas. 368 Pág. ISBN: 8441528020. ISBN-13: 9788441528024.

Referencias Electrónicas

MANZANO David. 2007. Universidad Politécnica de Valencia.
URL: http://www.grc.upv.es/Software/maya/Memoria.pdf

GARCÍA FERNÁNDEZ Néstor. 2006. Universidad de Oviedo, Tesis Doctoral, Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.URL: http://www.di.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf

WIKIPEDIA. 2012. Mesh networking. URL's:
http://en.wikipedia.org/wiki/Mesh_networking.
Http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica_Mesh

MESHDYNAMICS. 2012. The Smart Multi-Grid Solution for Public Networks. URL: www.mesdyanmics.com

LUGRO Mesh. 2008. Tecnología Mesh aplicada a redes WiFi comunitarias. URL: http://www.lugro-mesh.org.ar/doc/LUGRo-Mesh%20-%20texto%20charla%208vas%20JRSL.pdf

BÜTTRICH Sebastian. 2007. Büttrich.less.dk wire. Redes Mesh guía. URL: http://www.eslared.org.ve/tricalcar/13_es_redes_mesh_guia_v02%5B1%5D.pdf

SEVILLA Mesh. 2011. Orígenes de las redes Mesh II: Redes MANET y expansión de Wi-Fi. URL: https://sevillamesh.wordpress.com/tag/redes-mesh/

WIKIPEDIA. 2013. Red Inalámbrica mallada. Actualizada: 23 de abril 2012. URL: http://es.wikipedia.org/wiki/Red_inal%C3%Almbrica_Mesh

ALFÉREZ Antonio. 2012. Documento. IIC. Doctor Área de Telecomunicaciones: URL: www.aslam.es/files/381-187-Archivo/IIC.pdf?download=1

UDA. 2012. Página web de la Universidad del Azuay. El Campus y nuestros Organismos.URL: http://www.uazuay.edu.ec/campus/mapa.htm

LUGRO Mesh. 2010. Software Utilizado. [Fecha de consulta: septiembre 2014]. URL: http://lugro-mesh.org.ar/wiki/Software_Utilizado

WIKIPEDIA. 2014. Vector Distancias. URL: http://es.wikipedia.org/wiki/Vector_de_distancias

LINKSYS. 2005. Manual del Router Linksys.URL: https://broadband.sd.gov/Knowledge%20Base/Instructions%20and%20User%20Guides/User%20Guide%20Wireless%20Linksys%20Router%20WRT54GL.pdf

OPENWRT. 2013. Wireless Freedom. URL: https://openwrt.org/

ANEXO 1

UNA CONFIGURACIÓN SIMPLE OLSRD Y AD-HOC

Procedimientos para establecer una red ad-hoc.

Ingresamos al terminal del Linux

Procedemos antes que nada a ingresar como super usuario root con el comando:

su–

En mi caso mi contraseña esteban y obtenemos esto:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~#

Tratamos de ingresar el comando para que nuestra tarjeta inalámbrica quede configurada como modo Ad-hoc y ponemos el siguiente comando.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# iwconfig wlan0 mode Ad-hoc

Resultado: Error for wireless request “Set mode “(8b06):

SET invalid on device wlan0, operation not permitted.

Lo que se trata de hacer es que el adaptador de red reconozca el modo Ad-hoc y para esto tendremos utilizar los siguientes comandos.

Apagamos la interface inalámbrica con el siguiente comando:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig wlan0 down

Ponemos en el modo de conexión, el cual es nuestro objetivo ad-hoc con el siguiente comando:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# iwconfig wlan0 mode Ad-hoc

Nos sale una pantalla en blanco significa que hemos configurado bien nuestra tarjeta en Modo Ad-hoc.

Levantamos de nuevo la interfaz inalámbrica con el siguiente comando:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig wlan0 up

Antes de realizar estos pasos procedemos a deshabilitar redes inalámbricas que estén conectadas para no tener problemas.

Ahora ponemos el comando iwconfig y nos muestra lo siguiente.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# iwconfig

lo no wireless extensions.

eth0 no wireless extensions.

wlan0 IEEE 802.11bg ESSID:off/any

Mode:Ad-Hoc Frequency:2.412 GHz Cell: Not-Associated

Tx-Power=20 dBm

Retry long limit:7 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

Como podemos darnos cuenta no hay una celda asociada, pero si tiene parámetro de transmisión.

Escribimos el siguiente comando para poner nombre a la red:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# iwconfig wlan0 essid "Esteban"

Como resultado tenemos esto de abajo:

lo no wireless extensions.

eth0 no wireless extensions.

wlan0 IEEE 802.11bg ESSID:"Esteban"

Mode:Ad-Hoc Frequency:2.412 GHz Cell: Not-Associated

Tx-Power=20 dBm

Retry long limit:7 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

Ya tenemos un nombre Essid, pero no tenemos celda asociada, para esto hay queconfigurar manualmente la dirección IPV4, que se nos ocurra con el comando de abajo.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig wlan0 192.168.0.101

Ahora comprobamos que tengamos dirección IP en el interfaz wlan0.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig

Como no tenemos, procedemos a escribir el comando de abajo manualmente:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig wlan0 192.168.0.101

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ifconfig
eth0 Link encap:Ethernet direcciónHW 00:1d:72:70:65:51
ACTIVO DIFUSIÓN MULTICAST MTU:1500 Métrica:1
Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)
Interrupción:41 Dirección base: 0xa000

lo Link encap:Bucle local
Direc. inet:127.0.0.1 Másc:255.0.0.0
Dirección inet6: ::1/128 Alcance:Anfitrión
ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
Paquetes RX:388 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:388 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:0
Bytes RX:28272 (28.2 KB) TX bytes:28272 (28.2 KB)

wlan0 Link encap:Ethernet direcciónHW 00:1f:e2:a2:87:34
Dirección inet4:192:168:0:101 Netmask; 255:255:255:0
Dirección inet6: fe80::21f:e2ff:fea2:8734/64 Alcance:Enlace
ACTIVO DIFUSIÓN MULTICAST MTU:1500 Métrica:1
Paquetes RX:13 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:179 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:1000
Bytes RX:2235 (2.2 KB) TX bytes:43832 (43.8 KB)

El último paso es hacer ping para que haya una respuesta de transmisión por tiempo: Esta configuración repetimos con los otros computadores inalámbricos para ver si hay respuesta, y si la comunicación entre estos puede ser posible.

192.168.0.101 Es la dirección IP que me asigne Esteban:
192.168.0.102 Es la dirección IP del otro computador llamado Víctor:
192.168.0.103 Es la dirección IP del tercer computador llamado Carlos:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ping 192.168.0.102

Pinging 192.168.102 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 Ttl 128 15ms

Reply from 192.168.0.101: bytes=32 Ttl 128 1ms

Reply from 192.168.0.101: bytes=32 Ttl 128 4ms

Reply from 192.168.0.101: bytes=32 Ttl 128 4ms

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~# ping 192.168.0.102 –c 10

Este comando nos despliega una lista de 10 muestras.

Esto solo es para ejemplificar; si notamos que hay ping, la comunicación entre nodos(computadores) es posible y se puede establecer la misma.

Gráficos demostrativos ***Fig. A1; Fig. A2.....Fig. A8.***

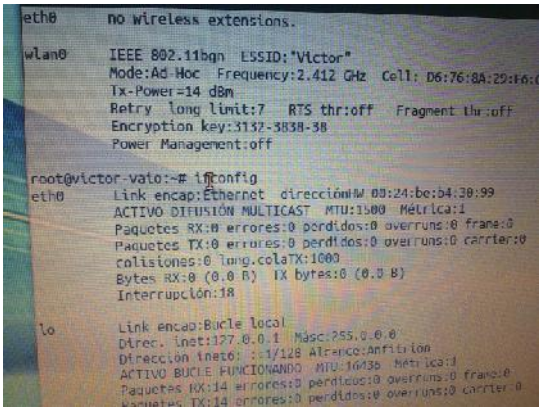


Fig. A1: Interfaz Gráfica de Red Víctor.

Fig. A2: Conexiones ESSID de Red.

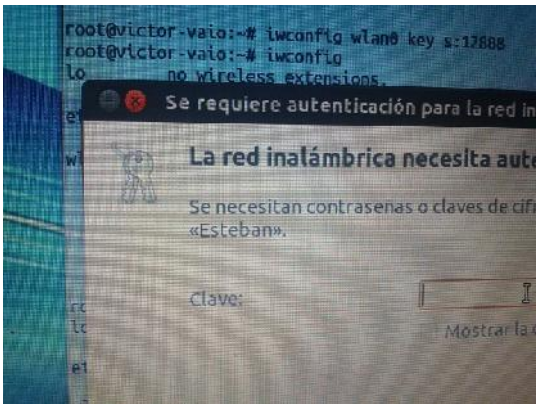


Fig. A3: Autenticación de Red Inalámbrica modo Ad-hoc Víctor.

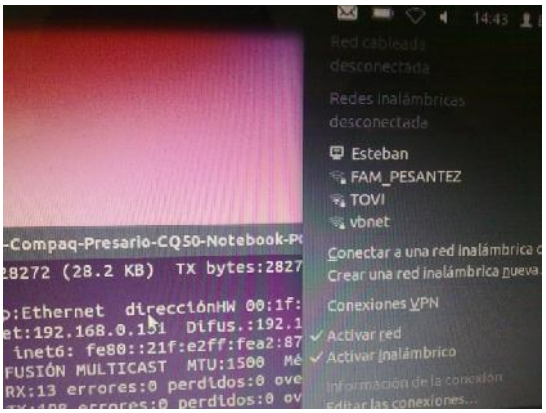


Fig. A4: Conexión de Terminal de Red Ad-hoc Esteban

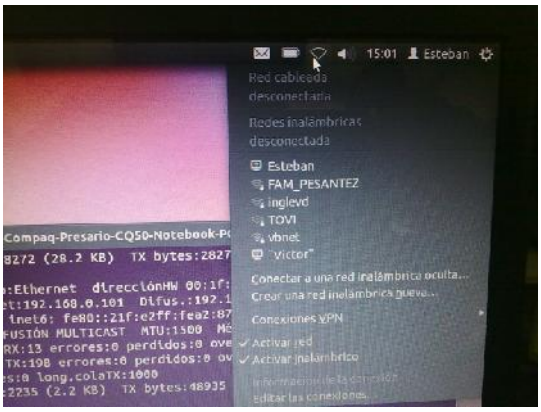


Fig. A5: Conexión Dual Terminales Ad-hoc Esteban - Víctor

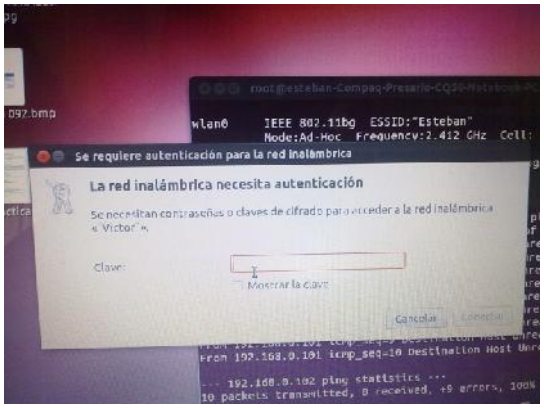


Fig. A6: Autenticación de Red Inalámbrica modo Ad-hoc Esteban.

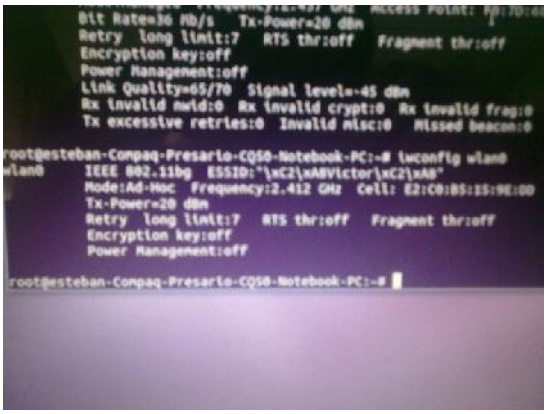


Fig. A7: Interfaz Gráfica de Red Esteban.

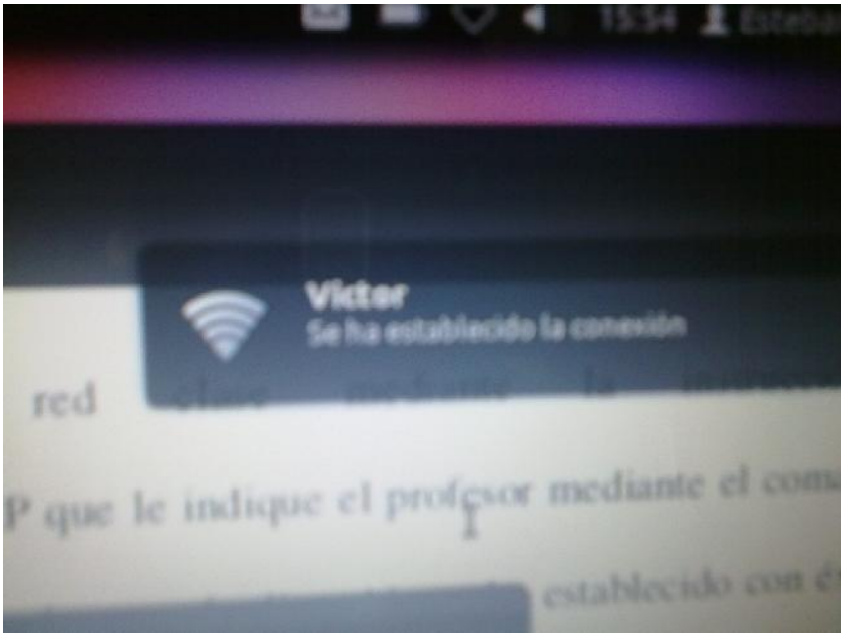


Fig. A8: Conexión establecida en Modo Ad-Hoc con terminal Víctor.

El objetivo era mostrar que si se podía conectarse a una red en modo Ad-hoc, y si pasa esto es porque se estableció la comunicación entre dos terminales, con esto es suficiente para conectarse a otros solo sería de hacer las respectivas configuraciones, pero no olvidarse de dar ping para ver que está sucediendo y así dar el acceso por medio de una clave personal de la red que estemos creando. **Fig. A8.**

ANEXO 2:

SIMULACIÓN DE LA RED MESH CON PROTOCOLO D.S.D.V

Procedemos antes que nada a ingresar como super usuario root con el comando:

su -

En mi caso mi contraseña esteban y obtenemos esto:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~#

Se accede al directorio con el comando cd al que deseamos iniciar la simulación:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:~#

cd /home/esteban/Simulador/Simulacion/

Una vez que estamos en el directorio damos ls para ver que ficheros existen:

root@esteban-Compaq-Presario-CQ50-Notebook-PC:

/home/esteban/Simulador/Simulacion# ls

Y se despliega la siguiente pantalla.**Fig. A9**:

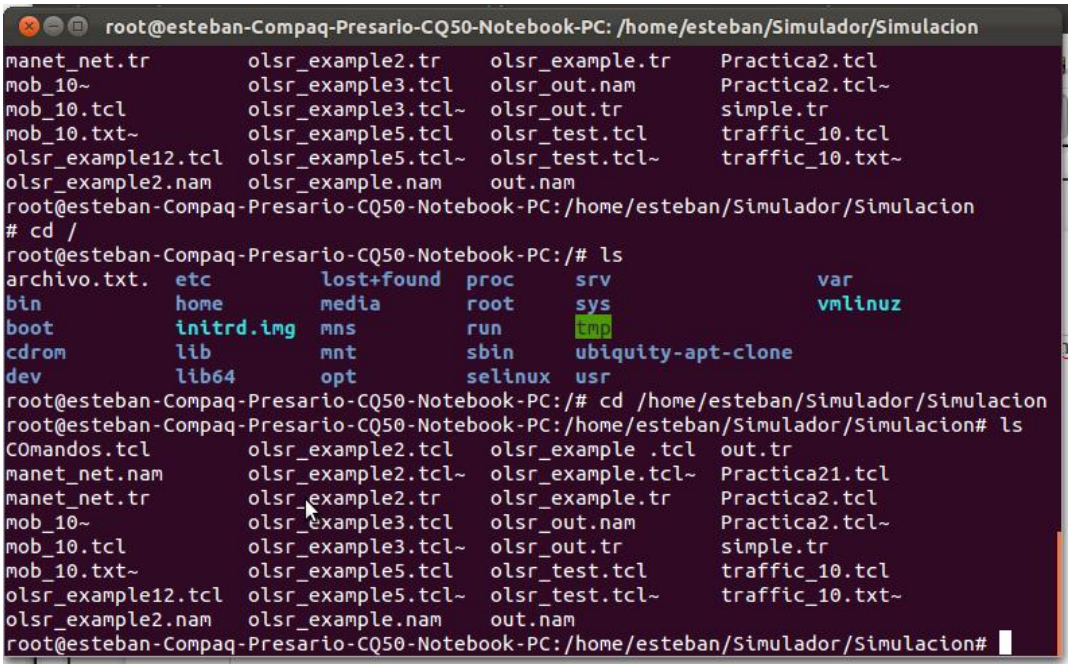


Fig. A9: Pantalla del Terminal de Linux Ubuntu 11.10.

El archivo para la simulación es el que dice practica2.tcl.

Si queremos modificar el archivo tenemos que operar el comando siguiente: gksudo nautilus con este podemos accesar a los archivos que están protegidos contra escritura y hacer las modificaciones correspondientes.

A continuación detallo el Scrib que se llama Practica2.tcl y al que se procede haciendo modificaciones en sus parámetros.

```
==========================================================
# Definición de opciones
set val(chan)   Channel/WirelessChannel          ;# tipo de canal
set val(prop)   Propagation/TwoRayGround         ;# modelo de radio-propagación
set val(ant)    Antenna/OmniAntenna              ;# tipo de antena
set val(ll)     LL                               ;# tipo de capa de enlace
set val(ifq)    Queue/DropTail/PriQueue          ;# tipo de disciplina de cola
set val(ifqlen) 50                               ;# tamaño max de paquetes en la cola
set val(netif)  Phy/WirelessPhy                  ;# tipo de interface de red
set val(mac)    Mac/802_11                       ;# tipo de MAC
set val(rp)     DSDV                             ;# protocolo de rutado ad-hoc
set val(nn)     5                                ;# número de nodos móviles
set val(MNcoverage) 30.0                         ;# cobertura de los nodos
# Data Rate
# Tamaño de los paquetes UDP
Agent/UDP set packetSize_  1500
set val(pck) 1500                                ;# Tamaño de los paquete
set val(icbr) 0.005                              ;# Tamaño intervalo entre paquetes
# Energymodel
set opt(engmodel) EnergyModel
set opt(txPower) 2.15                            ;# transmitting power consumed in W
set opt(rxPower) 0.9                             ;# receiving power consumed in W
set opt(idlePower) 0.75                          ;# idle power consumed in W
set opt(initeng) 1000.0                          ;# Initial energy in Joules
# Up the data rate to 802.11b rates
Mac/802_11 set dataRate_ 11Mb
```

Disable RTS. This means that an RTS will only be sent for packets that are bigger than 3000 bytes, which should be never.

```
# If you want RTS/CTS on, then set this value to zero
Mac/802_11 set RTSThreshold_ 0
# Switch to the short preamble
Mac/802_11 set PreambleLength_ 72

# Antenna gain
Antenna/OmniAntenna set Gt_ 2
Antenna/OmniAntenna set Gr_ 2
# Programa Principal
# Se definen Variables Globales
set ns_ [new Simulator]
set tracefd [open simple.tr w]
$ns_ trace-all $tracefd
# Configuramos la topografía del escenario
set topo [new Topography]
$topo load_flatgrid 30 30

# Asignación parámetros básicos de las antenas de los nodos
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 2.0
Antenna/OmniAntenna set Gr_ 2.0
Phy/WirelessPhy set bandwidth_ 11Mb

# System Loss Factor
Phy/WirelessPhy set L_ 1.0
# Channel-13. 2.472GHz
Phy/WirelessPhy set freq_ 2.472e9
# Transmit Power (17dBm)
Phy/WirelessPhy set Pt_ 0.050118723
# Inicialización de los parámetros del interfaz radio de los nodos
Phy/WirelessPhy set CPThresh_ 10.0          ;# Collision Threshold
Phy/WirelessPhy set CSThresh_ 1.559e-11   ;# Carrier Sense Power;
Phy/WirelessPhy set RXThresh_ 3.652e-10   ;# Receive Power Threshold;
```

```
# Definición de la función para el cálculo de la potencia transmitida a partir de la
cobertura deseada
proc SetPt { coverage } {
set Gt [Antenna/OmniAntenna set Gt_]
set Gr [Antenna/OmniAntenna set Gr_]
setht [Antenna/OmniAntenna set Z_]
sethr [Antenna/OmniAntenna set Z_]
set RXThresh [Phy/WirelessPhy set RXThresh_]
set d4 [expr pow($coverage,4)]
set Pt [expr ($RXThresh*$d4)/($Gt*$Gr*$ht*$ht*$hr*$hr)]
return $Pt
}
Phy/WirelessPhy set Pt_ [SetPt $val(MNcoverage)] ; # asigna la potencia transmitida a
# partir de la función previamente definida

# Creamos God
create-god $val(nn)
# Creamos los nodos y la conexión entre ellos
# Se crean 5 nodos: node (0) y nodos(5)
set chan_13_ [new $val(chan)]
# Configuración de nodos
$ns_ node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-topoInstance $topo \
-channelType $val(chan) \
-energymodel $opt(engmodel) \
-initialEnergy  $opt(initeng) \
-txPower $opt(txPower) \
```

-rxPower $opt(rxPower) \
-agentTrace ON \
-routerTrace ON \
-macTrace ON \
-movementTrace OFF

for {set i 0} {$i < $val(nn) } {incr i} {
set node_($i) [$ns_ node]
$node_($i) random-motion 0 ;# deshabilita el movimiento aleatorio
}
$node_(0) set X_ 0.0
$node_(0) set Y_ 11.08
$node_(0) set Z_ 0.0
$node_(1) set X_ 10.81
$node_(1) set Y_ 11.08
$node_(1) set Z_ 0.0
$node_(2) set X_ 22.15
$node_(2) set Y_ 11.08
$node_(2) set Z_ 0.0
$node_(3) set X_ 10.81
$node_(3) set Y_ 0.0
$node_(3) set Z_ 0.0
$node_(4) set X_ 10.81
$node_(4) set Y_ 15.76
$node_(4) set Z_ 0.0

Se hace la conexión cableada del nodo 4 al 1 con un ancho de banda de 100 Mb y 10 ms de retraso y con un tipo de cola DropTail.

```
$ns_ duplex-link $node_(4) $node_(1) 100Mb 10ms DropTail
# Nivel Trasnporte
set udp0 [new Agent/UDP]
$ns_ attach-agent $node_(4) $udp0
set sink0 [new Agent/Null]
# Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(1) $sink0
```

```
# se conectan directamente la fuente con el destino
$ns_ connect $udp0 $sink0
# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ $val(pck)
$cbr0 set interval_ $val(icbr)
$cbr0 set rate_ 11mbps
# Asignación fuente de tráfico con su agente correspondiente
$cbr0 attach-agent $udp0
$udp0 set class_ 0


# Nivel Trasnporte
set udp1 [new Agent/UDP]
$ns_ attach-agent $node_(1) $udp1
set sink1 [new Agent/Null]
# Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(0) $sink1
# se conectan directamente la fuente con el destino
$ns_ connect $udp1 $sink1
# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr1 [new Application/Traffic/CBR]
$cbr1 set packetSize_ $val(pck)
$cbr1 set interval_ $val(icbr)
$cbr1 set rate_ 11mbps
# Asignación fuente de tráfico con su agente correspondiente
$cbr1 attach-agent $udp1
$udp1 set class_ 1
```

```
# Nivel Trasnporte
set udp2 [new Agent/UDP]
$ns_ attach-agent $node_(0) $udp2
set sink2 [new Agent/Null]
# Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(1) $sink2
# se conectan directamente la fuente con el destino
$ns_ connect $udp2 $sink2
# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr2 [new Application/Traffic/CBR]
$cbr2 set packetSize_ $val(pck)
$cbr2 set interval_ $val(icbr)
$cbr2 set rate_ 11mbps
# Asignación fuente de tráfico con su agente correspondiente
$cbr2 attach-agent $udp2
$udp2 set class_ 2

# Nivel Trasnporte
set udp3 [new Agent/UDP]
$ns_ attach-agent $node_(4) $udp3
set sink3 [new Agent/Null]
# Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(2) $sink3
#se conectan directamente la fuente con el destino
$ns_ connect $udp3 $sink3
# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr3 [new Application/Traffic/CBR]
$cbr3 set packetSize_ $val(pck)
$cbr3 set interval_ $val(icbr)
$cbr3 set rate_ 11mbps
# Asignación fuente de tráfico con su agente correspondiente
$cbr3 attach-agent $udp3
$udp3 set class_ 3
```

```
# Nivel Trasnporte
set udp4 [new Agent/UDP]
$ns_ attach-agent $node_(2) $udp4
set sink4 [new Agent/Null]
# Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(3) $sink4
# se conectan directamente la fuente con el destino
$ns_ connect $udp4 $sink4
# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr4 [new Application/Traffic/CBR]
$cbr4 set packetSize_ $val(pck)
$cbr4 set interval_ $val(icbr)
$cbr4 set rate_ 11mbps
# Asignación fuente de tráfico con su agente correspondiente
$cbr4 attach-agent $udp4
$udp4 set class_ 4

# Nivel Trasnporte
set udp5 [new Agent/UDP]
$ns_ attach-agent $node_(3) $udp5
set sink5 [new Agent/Null]
#Se asigna el comportamiento al nodo específico
$ns_ attach-agent $node_(4) $sink5
# se conectan directamente la fuente con el destino
$ns_ connect $udp5 $sink5

# Nivel Aplicación
# Creación fuente de tráfico CBR
set cbr5 [new Application/Traffic/CBR]
$cbr5 set packetSize_ $val(pck)
$cbr5 set interval_ $val(icbr)
$cbr5 set rate_ 11mbps
```

```
# Asignación fuente de tráfico con su agente correspondiente
$cbr5 attach-agent $udp5
$udp5 set class_ 5
# Tiempo de simulación en los nodos.
$ns_ at 160.0 "$node_(4) label \"Origen2\""
$ns_ at 160.0 "$node_(3) label \"Destino2\""
$ns_ at 160.0 "$node_(2) label \"Destino2\""
$ns_ at 160.0 "$node_(1) label \"Origen1\""
$ns_ at 160.0 "$node_(0) label \"Destino1\""
# Temporización de la simulación
$ns_ at 0.1 "$cbr0 start"
$ns_ at 0.2 "$cbr1 start"
$ns_ at 0.3 "$cbr2 start"
$ns_ at 0.4 "$cbr3 start"
$ns_ at 0.5 "$cbr4 start"
$ns_ at 0.6 "$cbr5 start"
# Definimos en que instante se acaba la simulación
for {set i 0} {$i < $val(nn) } {incr i} {
$ns_ at 60.0 "$node_($i) reset";
}
$ns_ at 600.0001 "stop"
$ns_ at 600.0002 "puts \"NS EXITING...\" ; $ns_ halt"
proc stop {} {
global ns_ tracefd
$ns_ flush-trace
close $tracefd
}
puts "Empezando simulación..."
$ns_ run
```

Procedemos a arrancar la simulación con el comando ns por ejemplo: ns nombre del archivo Scrib a simular.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:

cd /home/esteban/Simulador/Simulacion# ns Practica2.tcl

Y tenemos como resultado lo que sale en la pantalla siguiente**Fig. A10**:

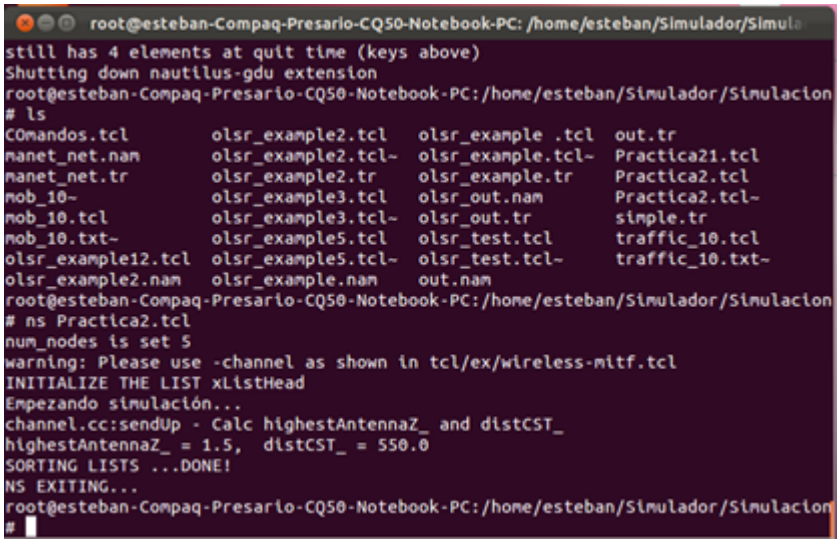


Fig. A10: Resultado de la simulación con el comando Ns

Esta pantalla demuestra que sí pudo completar la simulación y que no existieron errores. Ahora el siguiente paso es copiar ese archivo tipo Scrib para poder sacar la información de la simulación de los nodos que me propuse 5 nodos conectados en forma de topología MESH con el protocolo D.S.D.V.

Para eso se tiene que insertar el siguiente comando gksudo nautilus este hace que los archivos con protección de escritura se desprotejan y se puedan copiar debido a que el destino donde se encuentra el archivo está protegido y no puede ser copiado directamente.

root@esteban-Compaq-Presario-CQ50-Notebook-PC:

/home/esteban/Simulador/Simulacion# gksudo nautilus

Y se obtiene la siguiente pantalla a continuación **Fig. A11**:

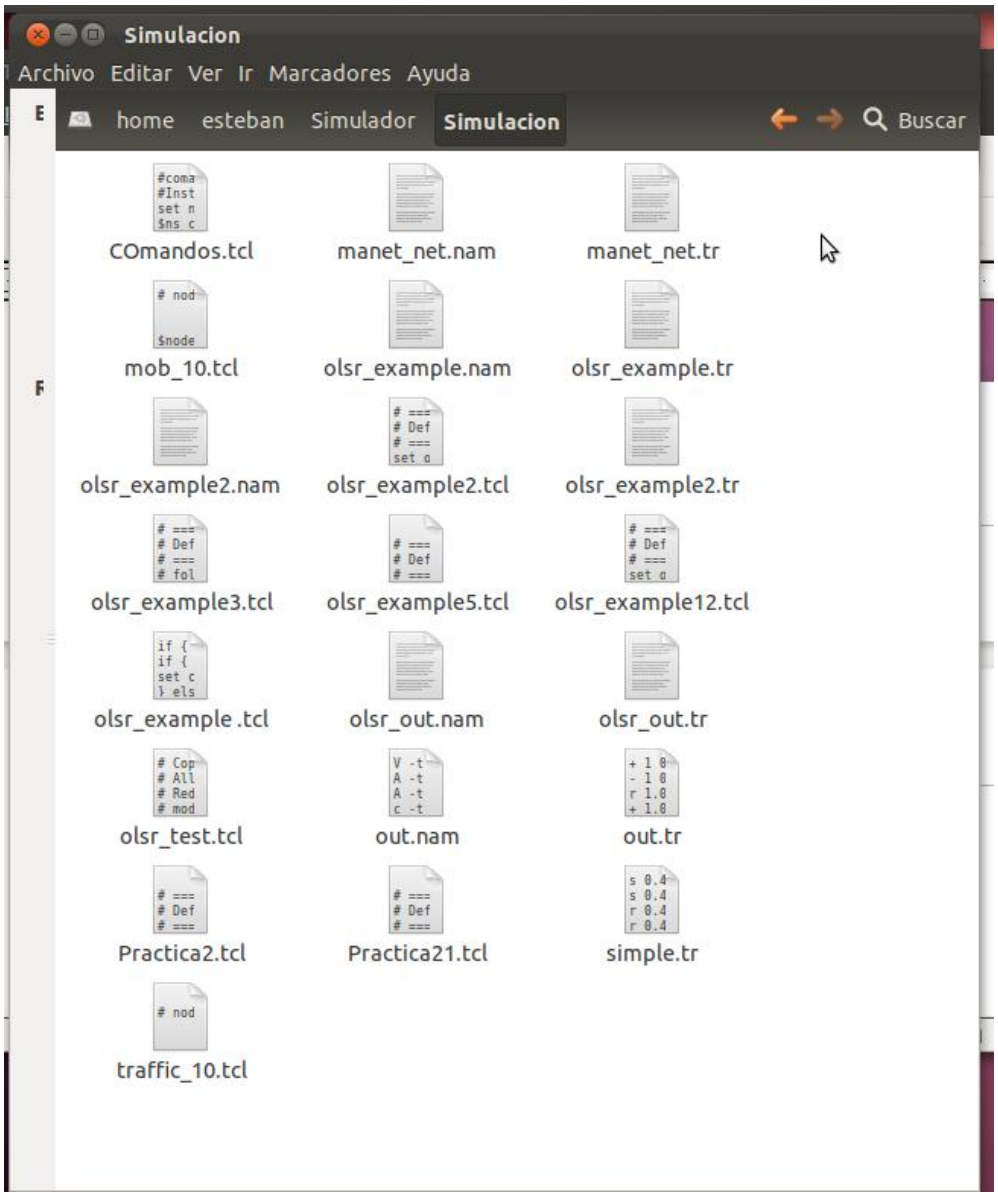


Fig. A11: Desprotección del Archivo Practica2.tcl

En donde se encuentra el archivo de simulación que se llama Practica2.tcl este archivo como se pueden apreciar ya no está con candado.

Lo cual permite en ese momento modificar y copiar para ser simulado con el Programa NSWireless.exe que se instaló en Windows 7 debido a que la información que se obtiene del archivo es procesada con dos tipos de archivos el tcl, y el archivo de traza .tr.

Estos dos utilizan el programa el primero tcl hace que se obtenga los nodos en un mapa virtual donde se puede apreciar los puntos de acceso con coordenadas, y el otro el tr hace que se den los resultados de simulación para poder medir los parámetros de interés como el throughput, perdidas, y el efecto jitter **Fig. A12**.

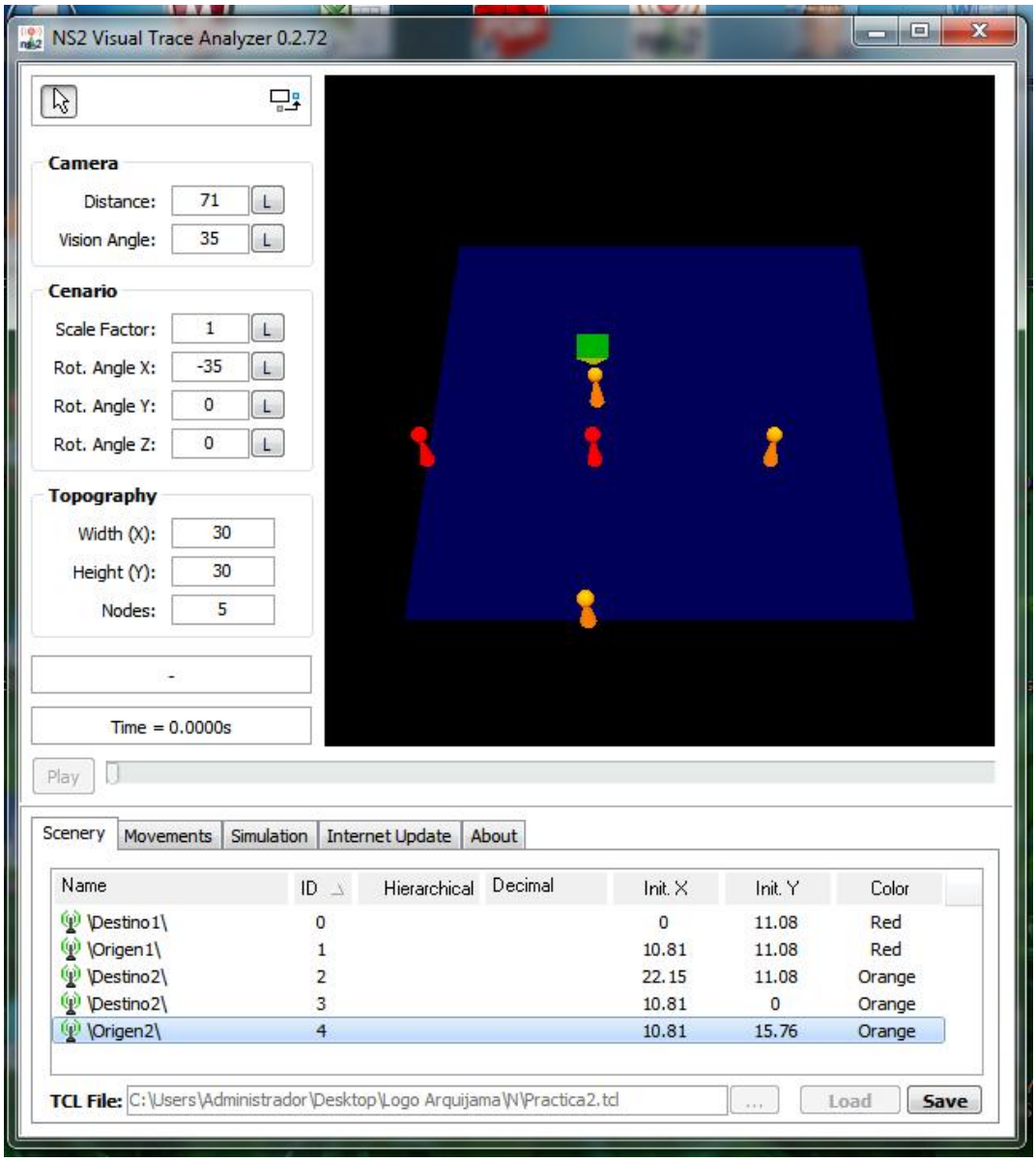


Fig. A12: Pantalla Simulación NS2 Visual Trace Analyzer 0.2.72

Cargando la simulación:

Se carga el archivo, primero se busca donde se guardó debido a que tengo dos sistemas instalados en el computador Linux Ubuntu 11.11 y Windows 7. El Scrib se simula en Linux es un archivo .tcl que contiene toda la programación para que este funcione.

El archivo .tr está cargándose en el Visual Trace Analyzer como se puede apreciar en la **Fig. A13:**

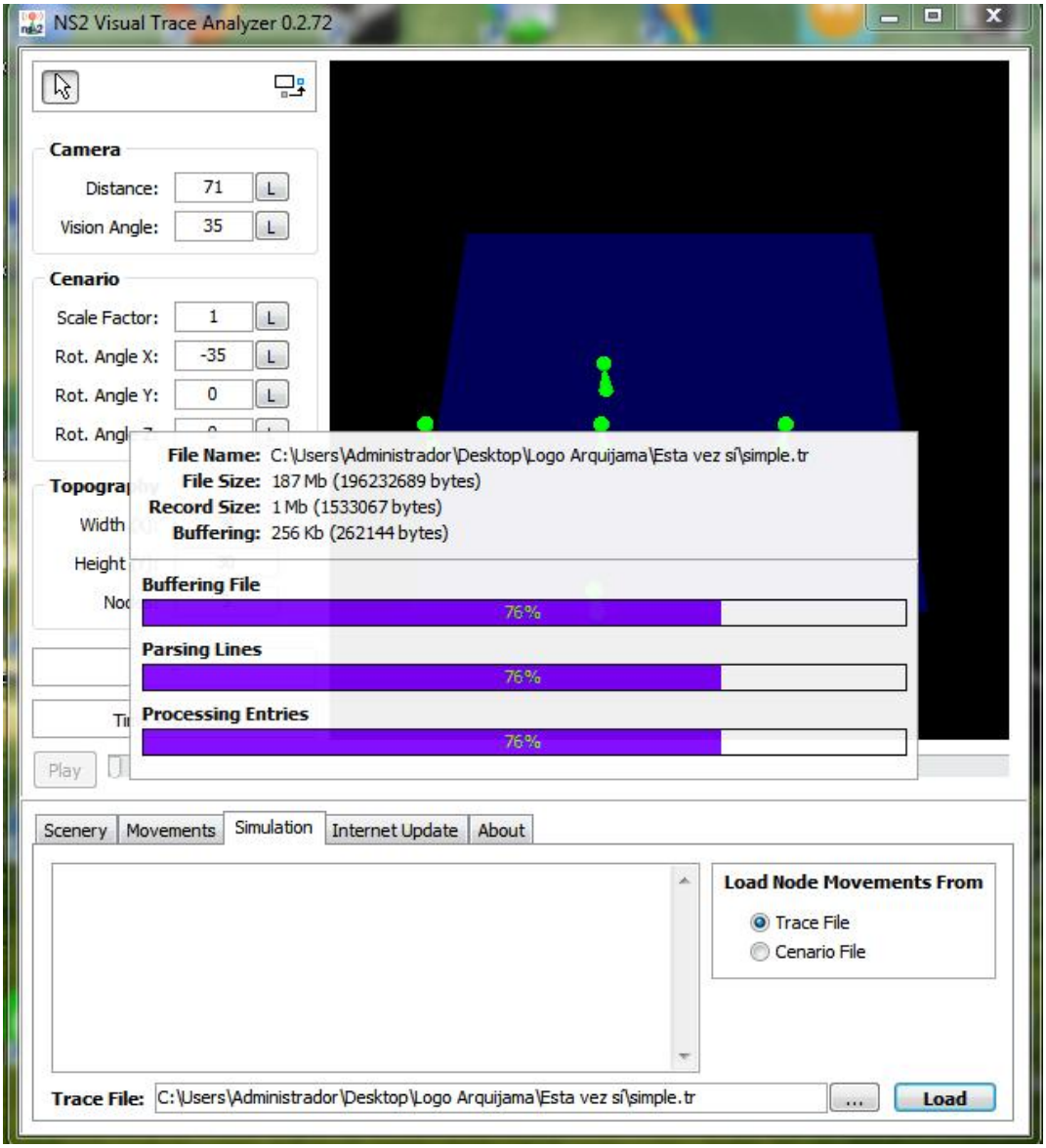


Fig. A13: Simulación Cargada de los archivos .tr y .tcl.en Windows 7.

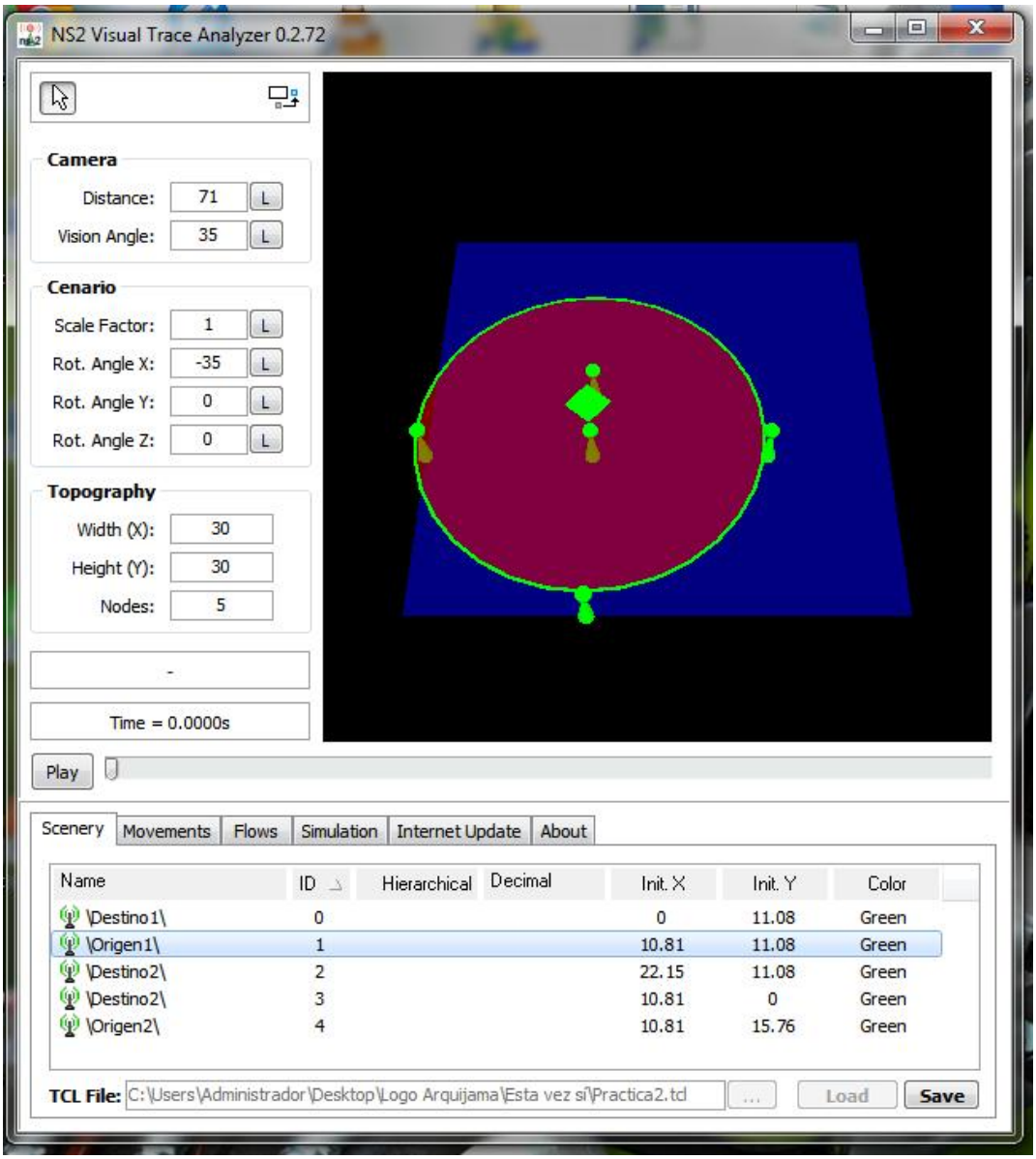


Fig. A14: Pantalla Cobertura medida en metros del nodo 1.

Según se nota la cobertura de los nodos **Fig. A14** se puede medir fácilmente debido a que se denota las áreas de cobertura y lo minino que puede tener es el Nodo Origen 1 es 11 metros aproximadamente para cubrir el nodo Destino 1 que corresponde al nodo 0 que se desea transmitir y es así como se estableció la topología.

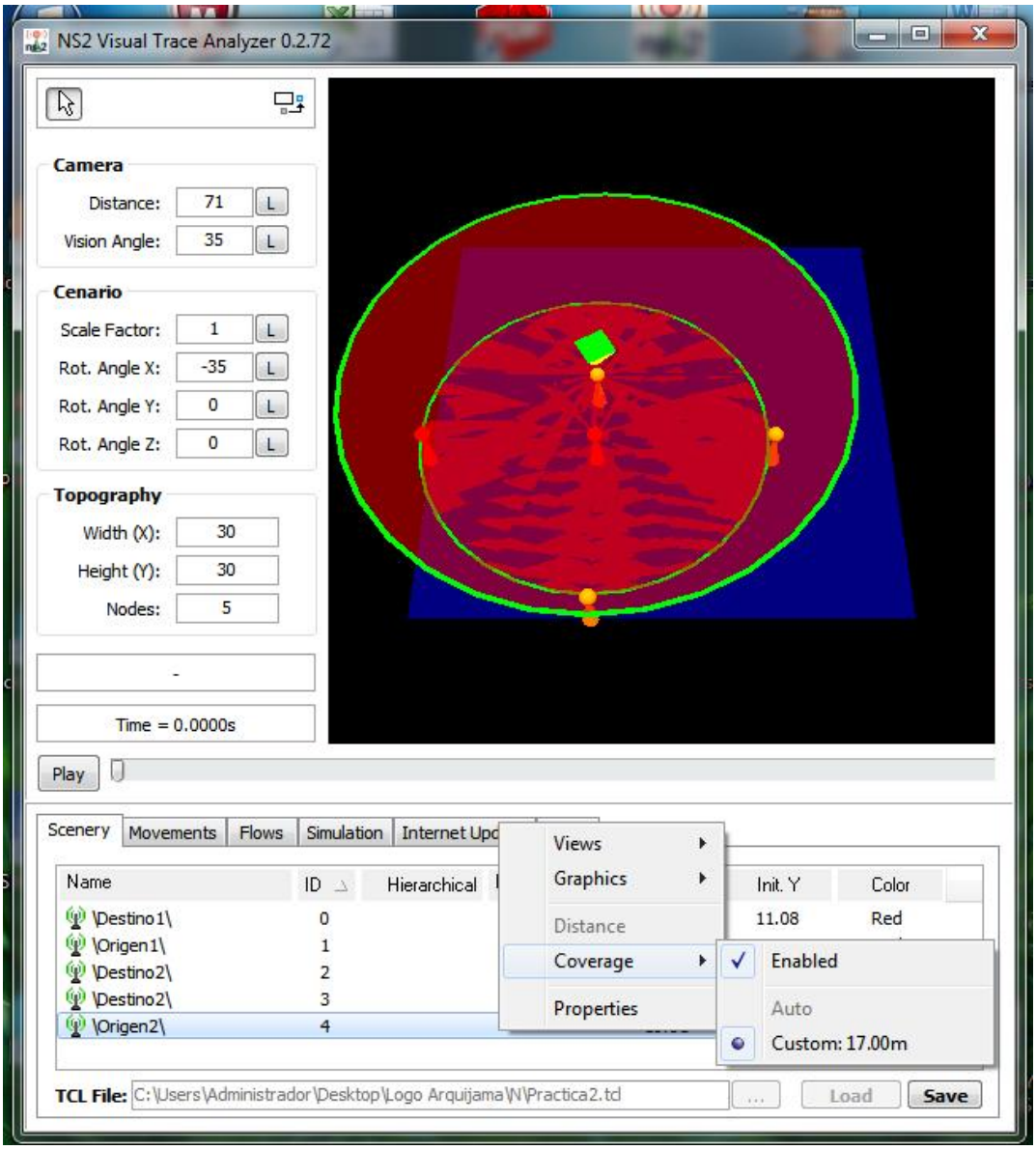


Fig. A15: Cobertura del nodo5 medida en metros.

Según se nota la cobertura de los nodos **Fig. A15** se pude medir fácilmente debido a que se denota las áreas de cobertura y lo minino que puede tener es el Nodo Origen 2 es 17 metros aproximadamente para cubrir los nodos Destino 2 correspondiente al nodo 3,4 que se desea transmitir.

Una vez obtenido los resultados se hace una estadística para ver qué cantidad de información circulo por la red en cada nodo, áreas de cobertura de los nodos y el respectivo análisis de los datos obtenidos.

Los resultados arrojados de cobertura **Fig. A16** que nos da el programa son 47 m redondeados según los cálculos y aplicado el modelo de telecomunicaciones que se obtuvo en el archivo Scrib Practica2.tcl con una ganancia en nuestro sistema de 2 en la antena receptora y trasmisora. Tx, Tr.

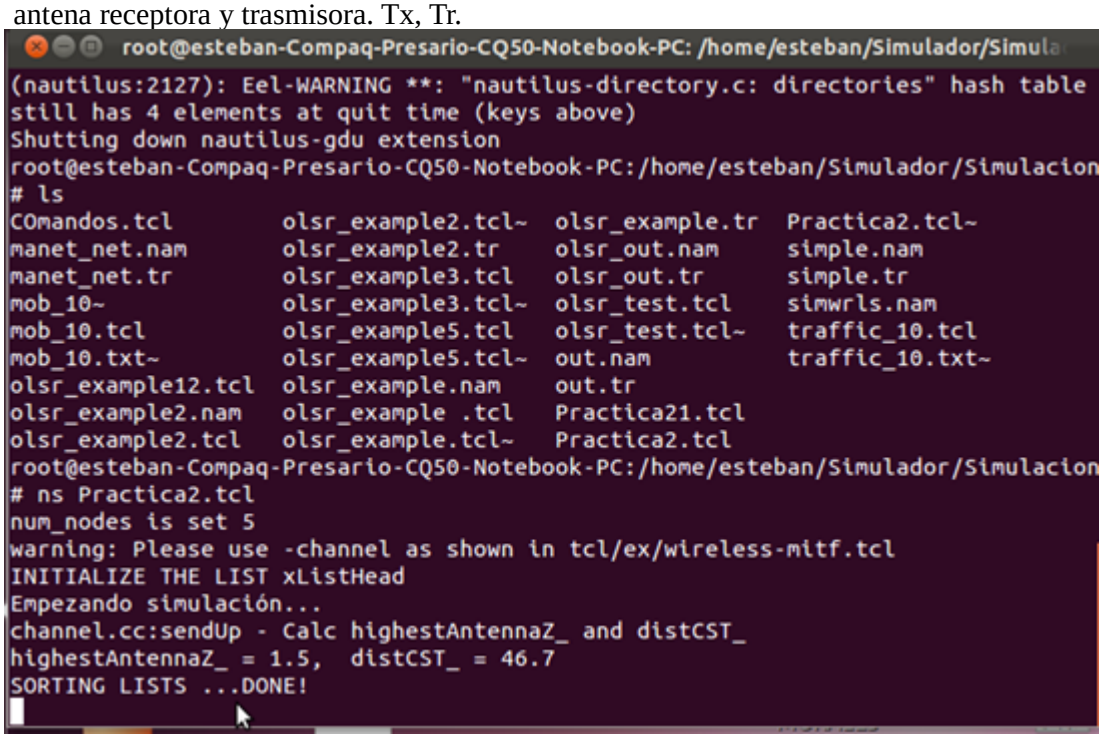


Fig. A16: Resultado de la distancia de Cobertura con NS2.

Haciendo la variación de la variable ganancia altera al sistema modificando la distancia de cobertura, y la Potencia Requerida varia. **Tabla A1.**

Ganancia Antena Transmisor	Ganancia Antena Receptor	Distancia de la Cobertura Requerida.	Distancia Calculada por el sistema	Potencia requerida a partir de su distancia de Cobertura(Pt)
1	1	30 m	74,0 m	0,0584 mWatts
2	2	30 m	47,6 m	0,146 mWatts
6	6	30 m	26,9 m	1,6222 mWatts
10	10	30 m	20,9 m	0,584 uWatts

Tabla A1: Resultados Calculados de Potencia Vs. Distancia Requerida de Cobertura.

Estos valores se basan en la Ecuación de Friis, está puesta en el archivo tcl como una función que calcula la potencia requerida a partir de la distancia de cobertura que se tiene con las variables de radio de interface.

Si graficamos en el NS2 Visual trazer Analyzer **Fig. A17** la cobertura de 47 m nos damos cuenta que llega muy lejos pasándose del límite que es de 30 m de Radio de topografía, con los parámetros establecidos en el programa del scrib Practica2.tcl.

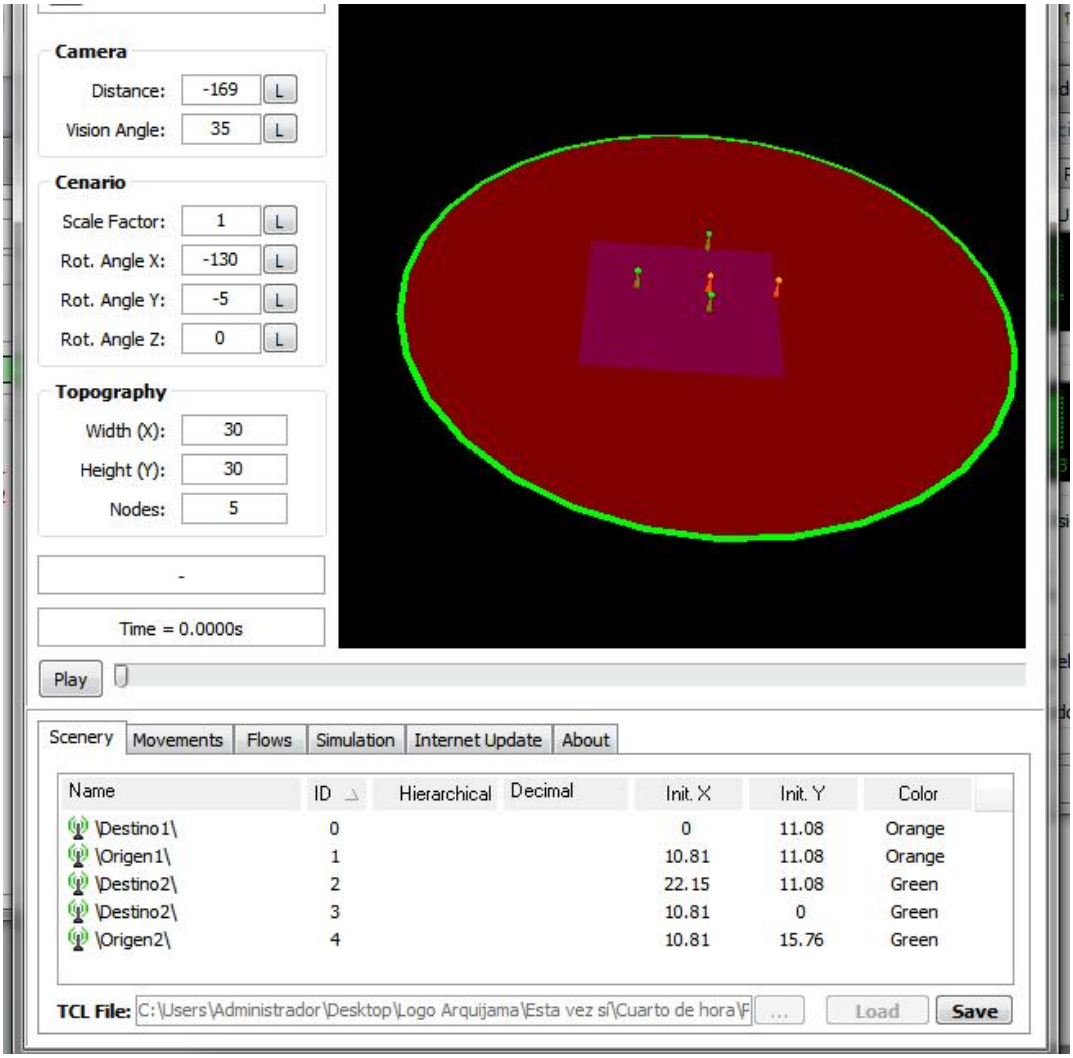


Fig. A17: Gráfico de Cobertura Virtual desde el Nodo Origen 1.

Observamos los datos enviados por mensajes en el nodo 0 Destino 1. **Fig. A18.**

La tasa promedio no supera los 32 bytes/s hasta los 160 segundos de simulación.

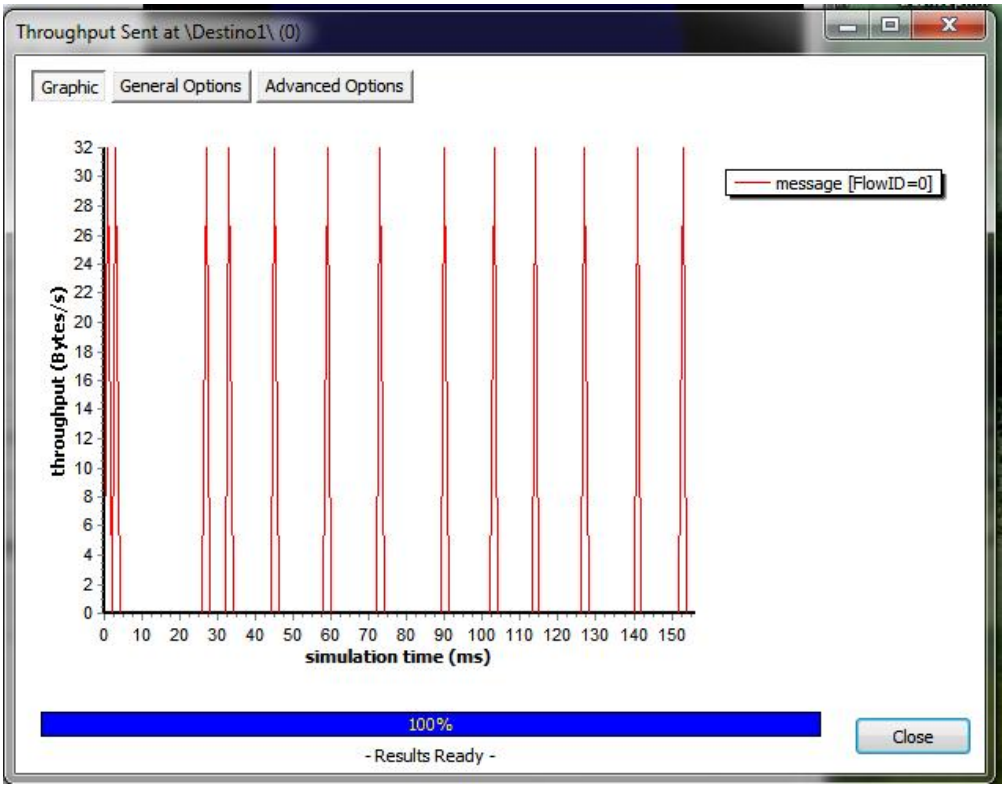


Fig. A18: Gráfico del Throughput de los mensajes Enviados al Nodo(0) "Destino1" transmitidos.

En esta **Fig. A19** podemos observar que en 60 paquetes tenemos un efecto jitter que varía entre los milisegundos esta puesto un valor de paquetes pequeño debido a que en nuestras gráficas este valor es casi cero y no se puede apreciar con todos los 1500 paquetes que me impuse.

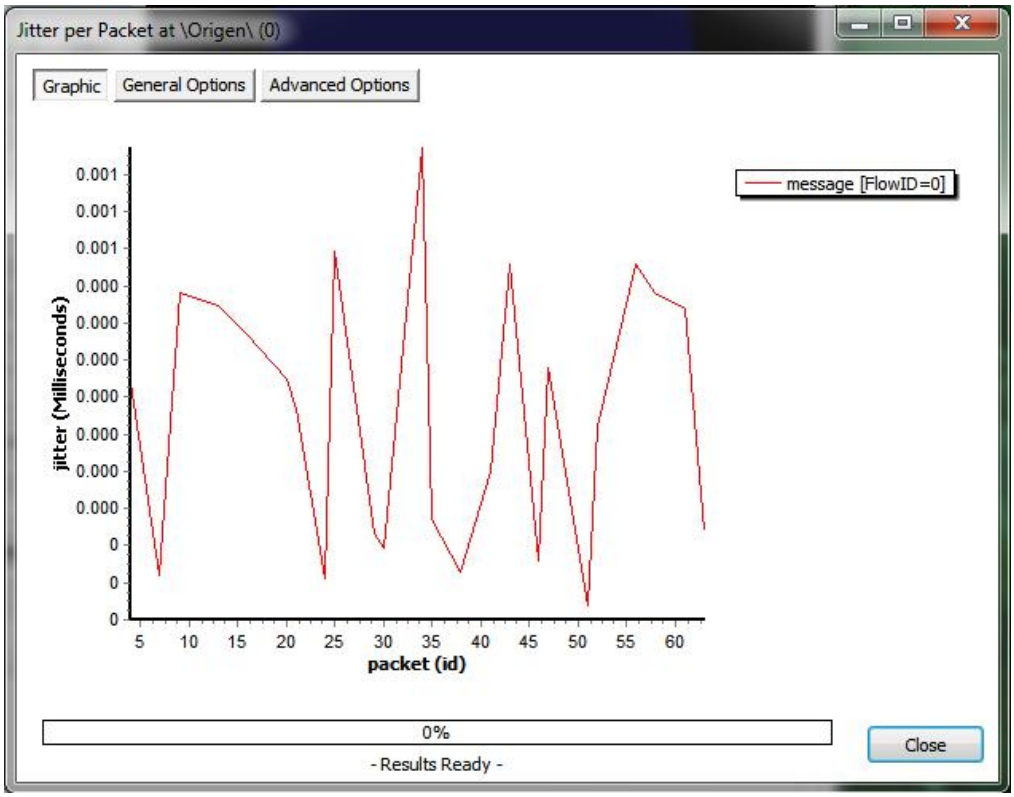


Fig. A19: Visualización del Efecto Jitter por Paquetes del Nodo(0) "Origen", 60 Paquetes.

La tasa promedio del nodo Origen 1 recibido es de 1,3 Megabytes/seg va subiendo desde 300 Kilobytes para los paquetes cbr. **Fig. A20.**

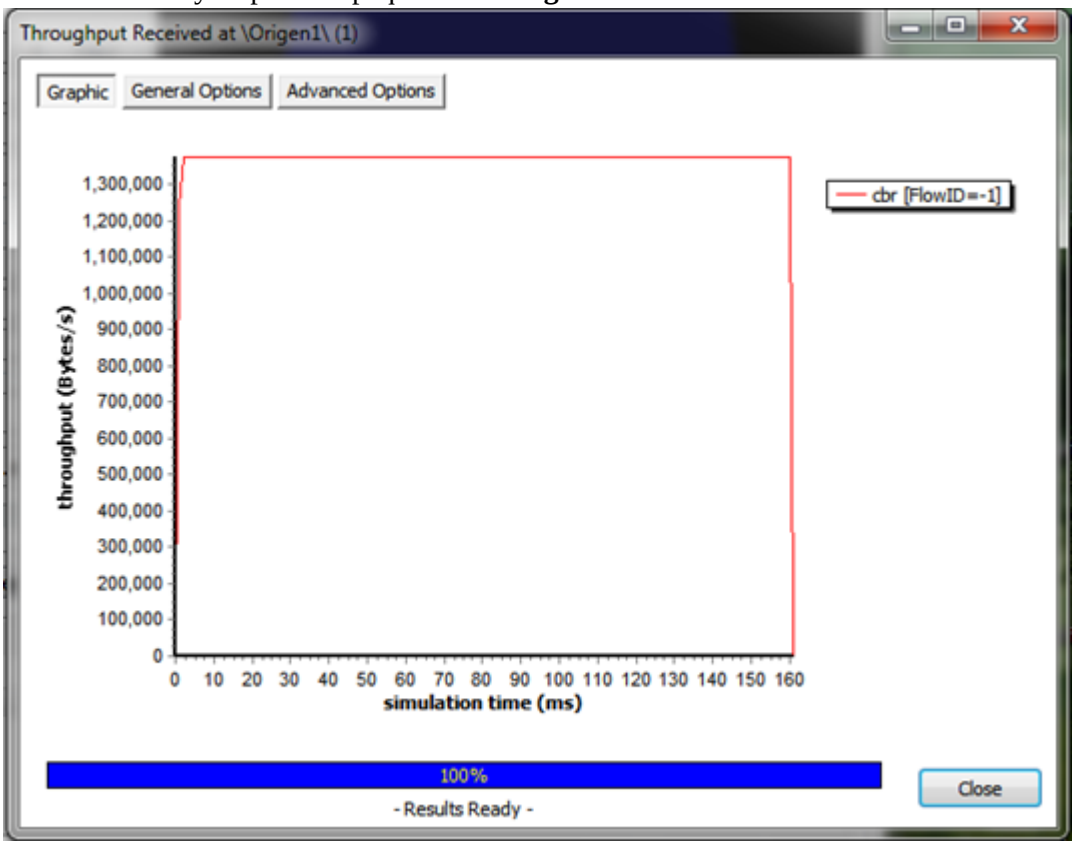


Figura A20: Medición del Throughput Recibido Nodo (1) "Origen1", norma b.

Esto demuestra que hubo un intercambio de información **Fig. A21**. Haciéndole un zoom la tasa promedio es de 1.35 Megabytes/seg hasta los 160 segundos de simulación.

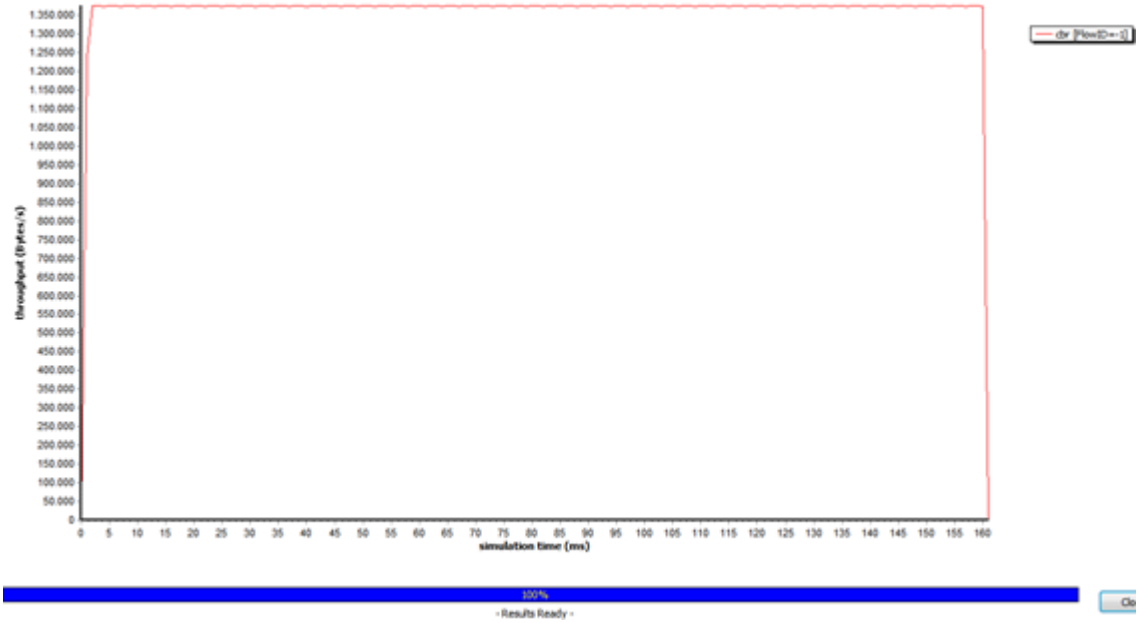


Fig. A21: Medición del Throughput de la Fig. A12.2 hecho Zoom, norma b.

La tasa promedio del nodo Destino2 recibido es de 1,35 Megabytes/seg va subiendo desde 50 Kilobytes para los paquetes cbr esta vez. **Fig. A22**.

Fig. A22: Medición del Througput Recibido Nodo(2) "Destino2" hecho Zoom, norma b.

La tasa promedio del nodo Destino1 recibido es de 1,35 Megabytes/seg va subiendo desde 50 Kilobytes para los paquetes cbr esta vez. **Fig. A23.**

Fig. A23: Medición del Througput Recibido Nodo(0) "Destino1" hecho Zoom, Norma b.

Haciendo la trasmisión de topología cableada la tasa promedio supera casi dos veces debido a que estamos conectando a los nodos 4 y 2. La taza es de 2,7 Megabytes/seg recibida del nodo 4. **Fig. A24.**

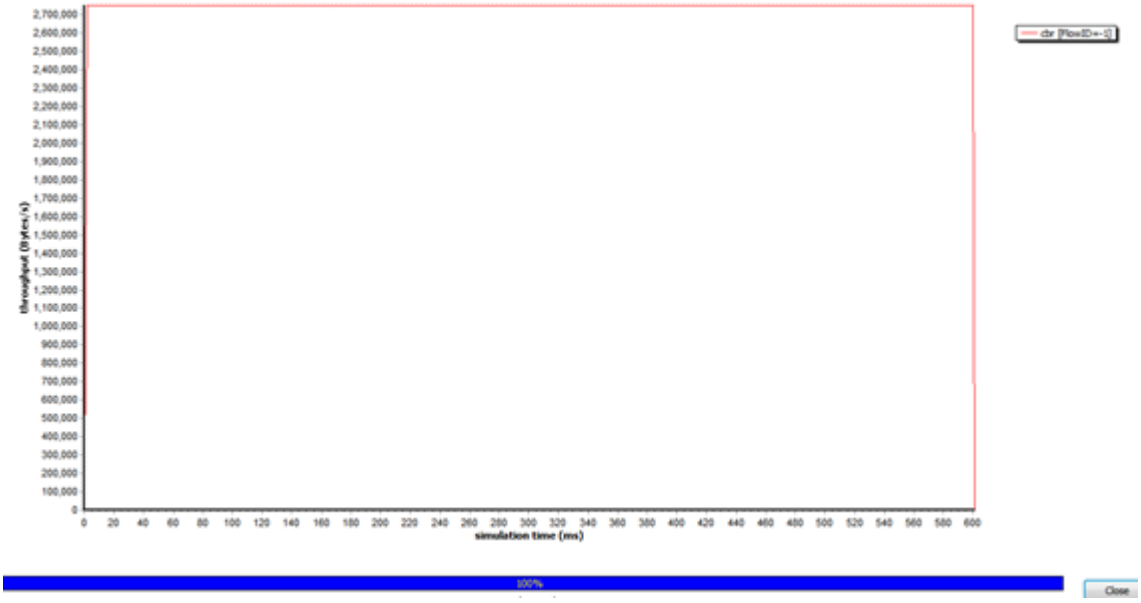


Figura A24: Medición del Througput Recibido Nodo (4) "Destino2" Cableada 4-2 hecho Zoom, Norma b.

Como se puede apreciar la Fig. **A25** y anterior está hecho un zoom para poder ver el valor.

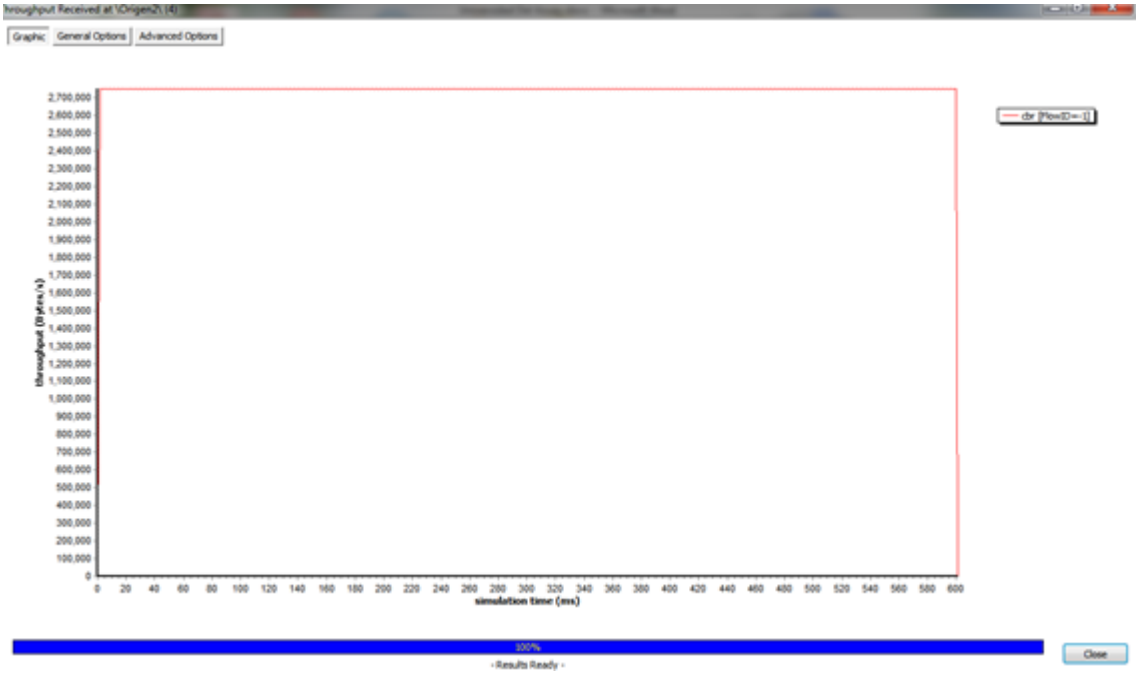


Figura A25: Medición del Througput Recibido Nodo (4) "Origen2" sin zoom. Norma b.

La información de las routas se puede observar en la **Fig. A26** que hubo rutas por donde se orientó esta topología de red propuesta tenemos Origen nodo 4 al nodo Destino 1 con 10999543 que son los 100 Megabytes impuestos.

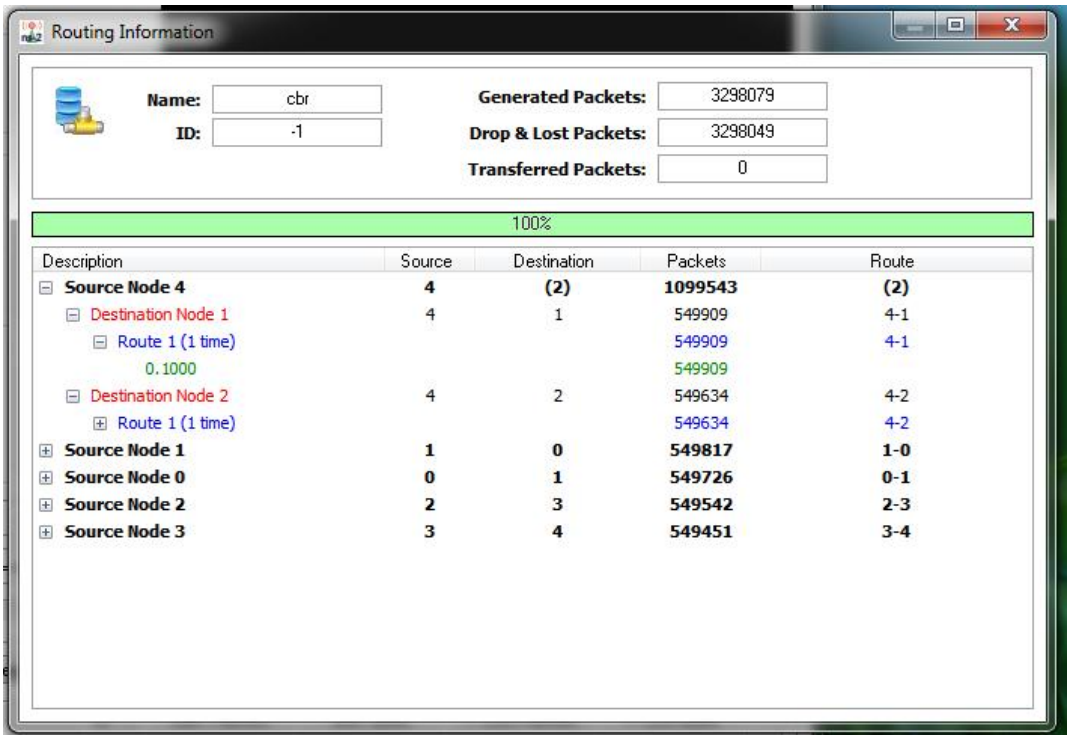


Fig. A26: Orientación de la Topología - Enlaces Lógicos.

Ahora se simulo con una cantidad de paquetes mayor ya que estamos transmitiendo con la norma g con 55 megabytes/seg, se puede observar una taza de 6,8 Megabytes/seg. para los paquetes cbr, con una ganancia de 2 para el transmisor y el receptor de la antena. **Fig. A27**.

Fig. A27: Medición del Througput Recibido Nodo (1) "Origen1" con Norma g.

Se simulo lo mismo solo que se cambió el tiempo de muestreo de los paquetes cbr de 0,0005 a 0,00005 seg y este fue el resultado. 7,5 Megabytes/seg. de CBR. **Fig. A28.**

Fig. A28: Medición del Througput Nodo (1) "Origen1" cambiado el tiempo de muestreo de los paquetes CBR Norma g.

Haciendo la trasmisión de topología cableada la tasa promedio supera casi dos veces debido a que estamos conectando a los nodos 4 y 2. La taza es de 3,5 Megabytes/seg recibida del nodo 4. Al variar la ganancia no varían las gráficas de muestreo solo se modifica la potencia mínima requerida para esas distancias y ganancias. **Fig. A29**.

Fig. A29: Medición del Througput Recibido Nodo (4) "Origen2" Cableada 4-2 con Norma g.

La misma simulación de arriba solo que se cambió el tiempo de muestreo de los paquetes cbr de 0,0005 a 0,00005 seg. Aumenta un poco más su transmisión. **Fig. A30.**

Fig. A30: Medición del Througput Recibido Nodo(4) "Origen2" cambiando el tiempo de muestreo de los paquetes CBR en norma g.

Ahora se muestra los paquetes generados, Bytes generados y Total de paquetes perdidos, junto con los Bytes perdidos también. **Fig. A31.**

Con norma b con transmisión de 11 Megabytes/seg.

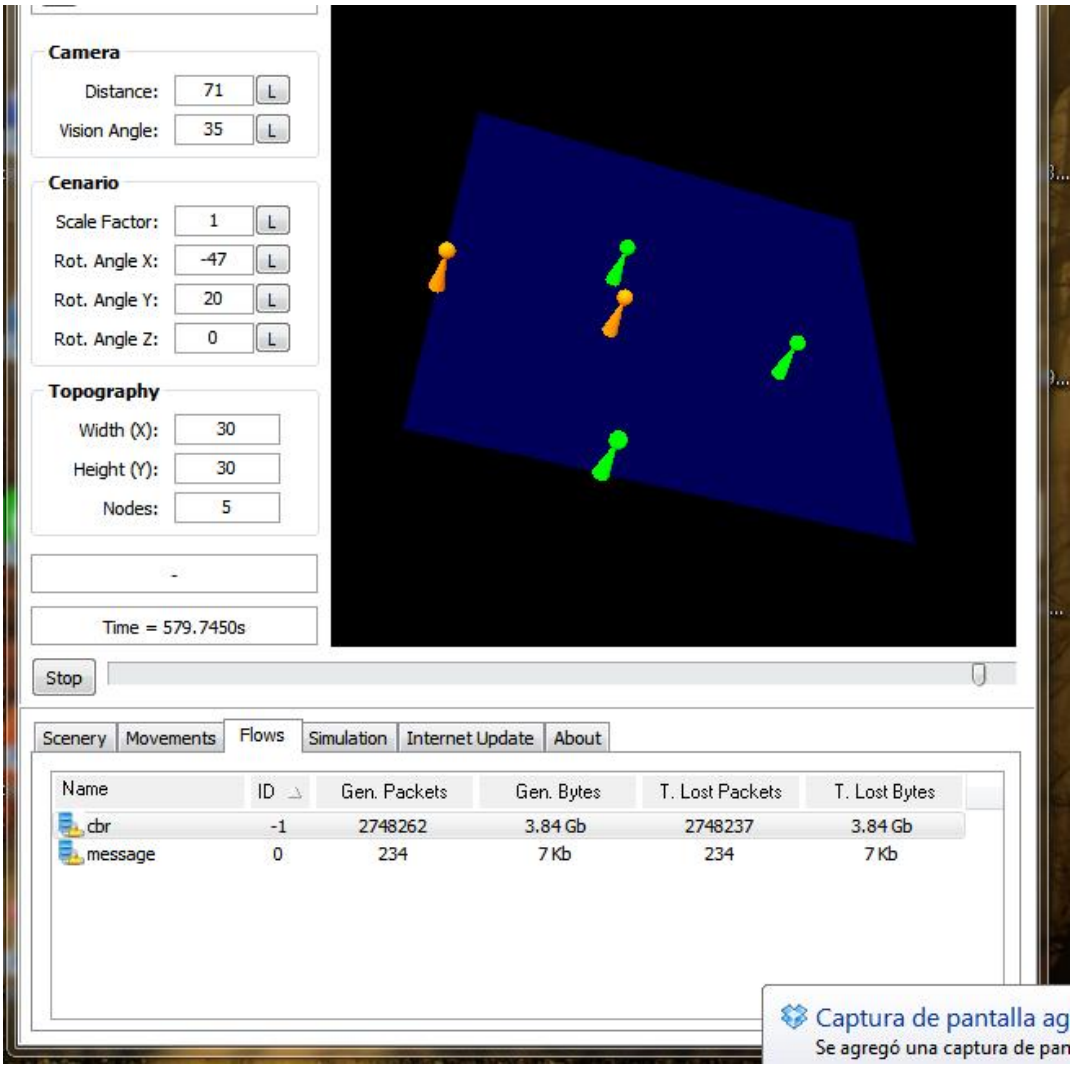


Fig. A31: Pantalla de Muestra de Paquetes, Bytes Generados; Total Paquetes Perdidos, Bytes CBR, y Mensajes con norma b.

Con norma g con transmisión de 55 Megabytes/seg. Se puede observar una variación de Los Bytes generados es mayor que la b.**Fig. A32.**

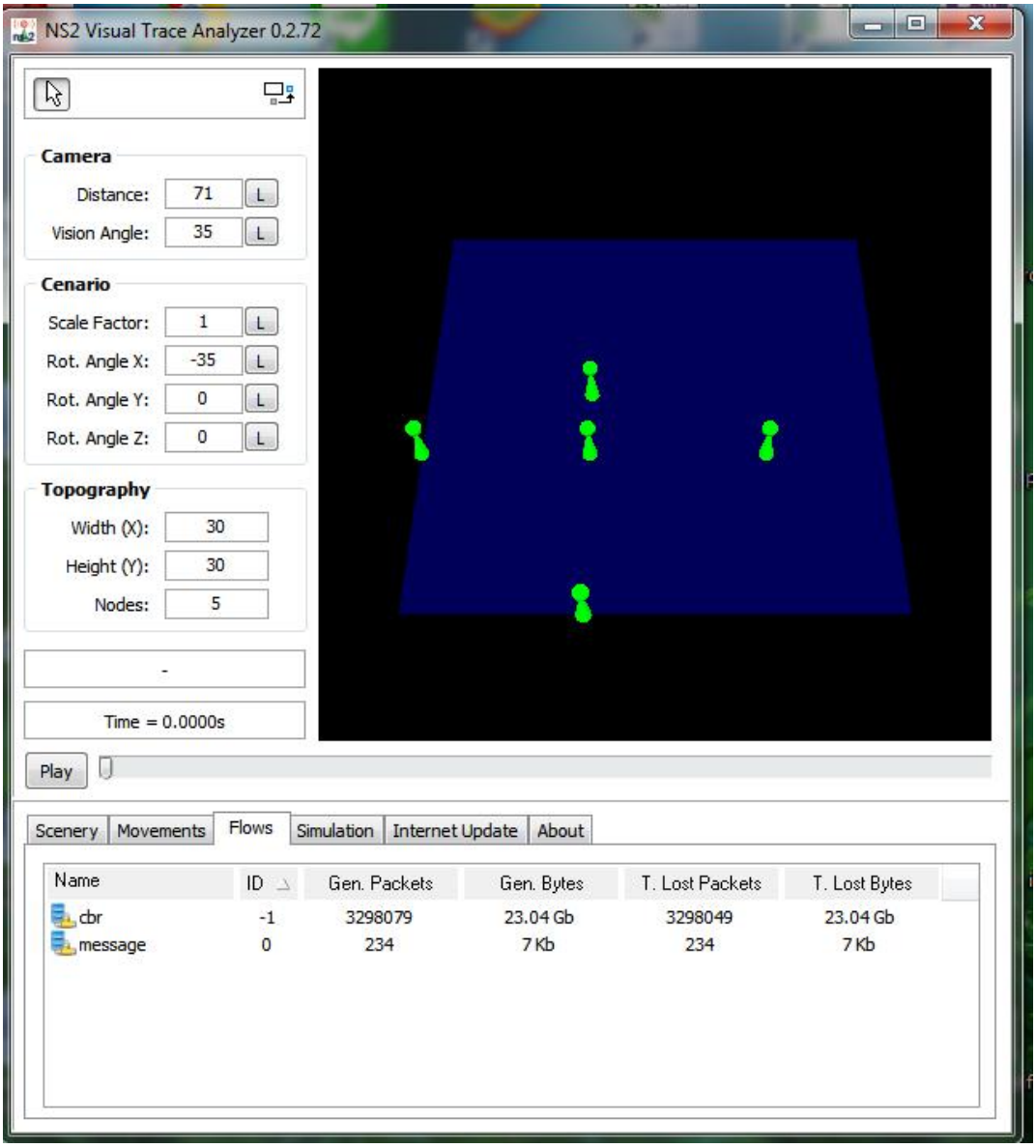


Fig. A32: Pantalla de Muestra de Paquetes, Bytes Generados; Total Paquetes Perdidos, Bytes CBR, y Mensajes con norma g.

Como último dato se hizo es la variación de Paquetes debido a que la cantidad para poder procesar los gráficos en cuestión va subiendo conforme se va aumentando el número de paquetes, es decir la cantidad de almacenamiento que se requiere es bastante elevada variando desde las megas hasta los gigabytes. Por ello tuve que hacer las prácticas en la Universidad con Ubuntu 13.10 y con un disco duro de casi 200 Gigabytes, lo cual fue factible realizar. **Fig. A33.**

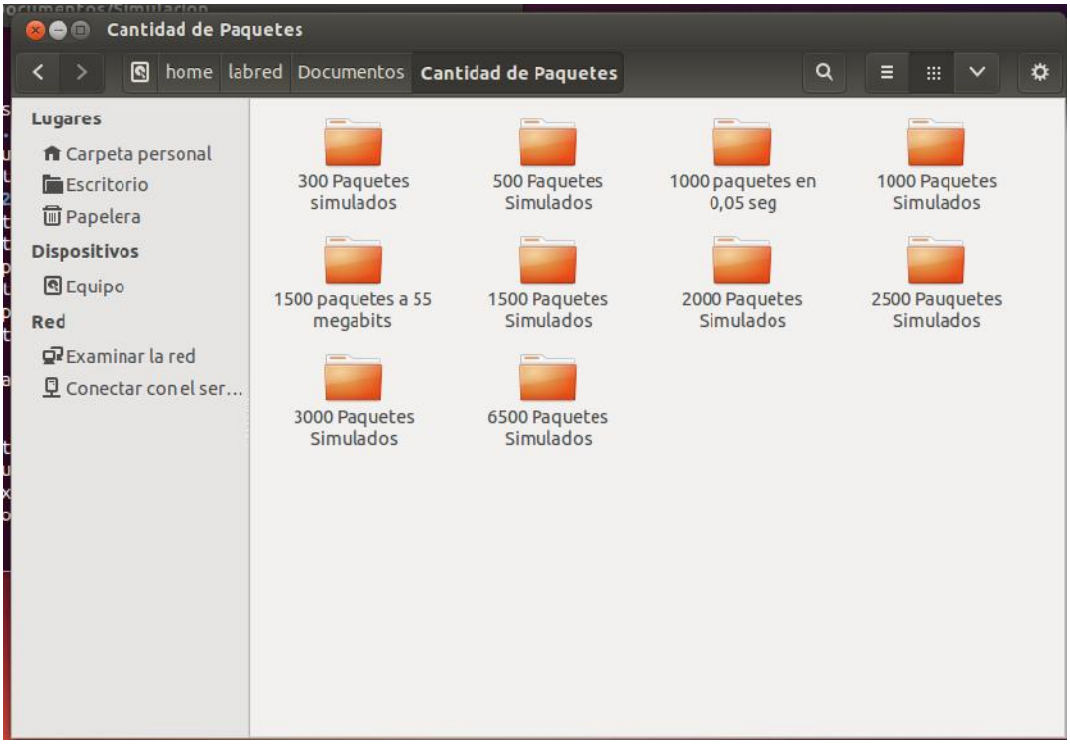


Fig. A33: Pantallazo Simulaciones de Carpetas de Almacenamiento de Paquetes.

Se puede observar el archivo de traza generado con un tamaño de 901,2 Mb, en norma g. **Fig. A34.**

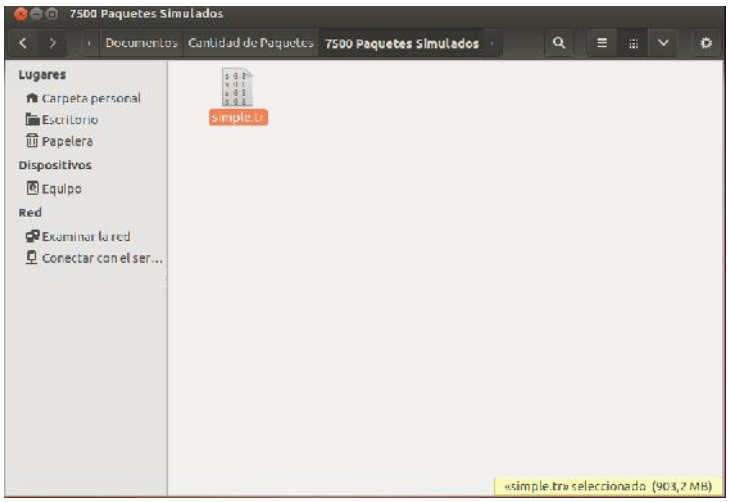


Fig. A34: Visualización del Pantallazo Archivo de Traza con norma g.

Se puede observar el archivo de traza generado con un tamaño de 4,6 Gb.

Para 3000 paquetes con norma b. Por esta razón como es tan grande el archivo de traza que al realizar la simulación en mi Laptop de escritorio los recursos de Ram se elevan imposibilitando su análisis.

El Ns2 Wireless.exe ya no puede examinar con exactitud los datos porque no los puede cargar lo hice de tal forma que se pueda observar o medir a un valor promedio menor que 1 Gb variando las variables dentro del límite para que se pueda extraer las gráficas de la simulación y se pueda observar sus fenómenos. **Fig. A35.**

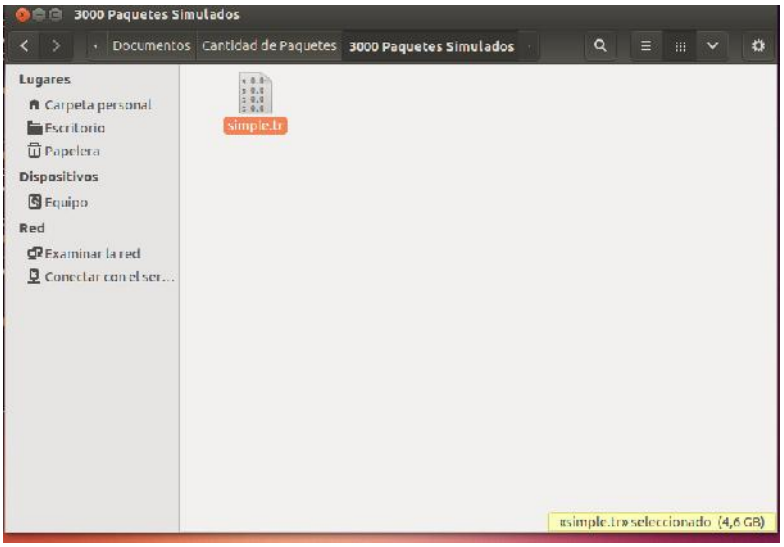


Fig. A35: Visualización del Pantallazo Archivo de Traza con 3000 paquetes simulados con norma b.

Se puede observar en la **Fig. A36** la simulación hecha en los Laboratorios de la Uda de Redes.

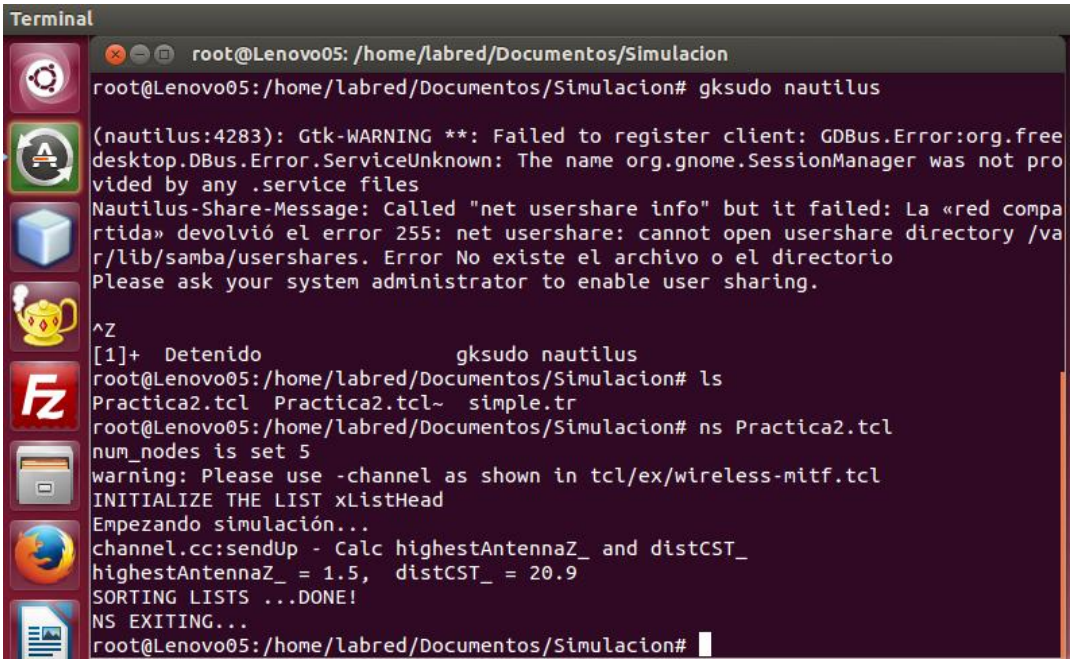


Fig. A36: Simulación Maquinas de los Laboratorios de Redes de Ciencia y Tecnología de la Universidad del Azuay.

ANEXO 3:

Explicación de cómo Funciona las variables y la programación en OTCL.

Pasos para escribir una simulación

Crear despachador

Crear registros de eventos

Crear los Componentes de Red

Agendar los eventos

Correr el simulador

Crear el despachador

set ns [new Simulator]

- Esto crea una instancia de la clase Simulator que será el encargado de manejar los eventos.
- Los métodos de dicha clase permiten armar la topología y configurar todo lo referente a la simulación.

Programar eventos y correr el simulador

La sintaxis de programación de eventos es la siguiente:

$ns at <tiempo><evento>

$ns es la variable \despachador" de la clase Simulator que se creó en el paso anterior

<evento> puede ser cualquier comando ns/tcl válido

$ns run

La línea anterior es la que corre el simulador, es la última línea del script.

Registro de Eventos

Es posible registrar todos los eventos que suceden en la simulación, generando un archivo de texto con toda lainformación:

$ns trace-all [open salida.out w]

$ns namtrace-all [open salida.nam w] - para visualización

También se pueden hacer trazas específicas y no de toda la simulación.

Tcl: Manejo de Variables y operaciones

Uso set para crear y asignarle un valor a una variable

```
set a 100
```

El signo de $ hace que el intérprete sustituya la variable por su valor

```
puts $a
```

Para realizar operaciones aritmétricas se utiliza el comando expr

```
expr 2*$a
```

Cadena contenida dentro de corchetes

La cadena se evalúa y se sustituye por el resultado obtenido.

```
set b [expr 2*$a]
puts $b
```

salida: 200

Cadena contenida entre comillas

```
set b \expr 2*$a"
puts $b
```

salida: expr 2*$a

obs: Para ejecutarla se requiere utilizar el comando eval

Tcl: Estructuras de control

for

```
for{set i 1}{$i <= 3}{incr i}
puts $i
}
```

while

```
set i 1
while{$i <= 3}{
puts $i
incr i
}
```

if

```
if{$i < 0 } {
puts "Negativo"
}else{
puts"Positivo o cero"}
```

Otros comandos Tcl útiles

Crear variables aleatorias

```
set gen [new RNG]
for{set j 1} {$j < $run}{incr} {
$gen next-substream}
set r [new RandomVariable/Uniform]
$r set min_ 0.0
$r set max_ 10.0
$r use-rgn $gen
```

Procedimientos

Un procedimiento se define de la siguiente manera:

```
proc nombreProc {arg1 agr2 ...g } ...
...
}
```

Agenda

Ejemplo 1: Hola Mundo

holaMundo.tcl

```
set ns [new Simulator]
$ns at 1 \puts \Hola Mundo!!!\" "
$ns at 1.5 exit
$ns run
```

Para correr el programa ejecutar:

ns holaMundo:tcl

Ejemplo 2: Red Cableada. **Fig. A37.**

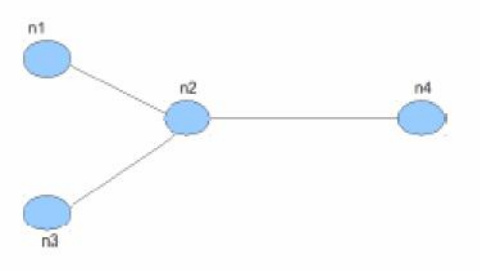


Fig. A37: Esquema gráfico de Topología Cableada.

Características a simular:

Trafico CBR/UDP desde n1 a n4

Trafico FTP/TCP desde n3 a n4

Enlace n1-n2 1Mbps, 2ms, DropTail

Enlace n3-n2 2Mbps, 2ms, DropTail

Enlace n2-n4 2Mbps, 3ms, DropTail

Visualizar el script ejemplo2.tcl

Ejemplo 2 cont

Definimos el despachador:

set ns [new Simulator]

Creamos los archivos de salida:

set nam [open salida:nam w]

$ns namtrace-all $nam

set tf [open salida:out w]

$ns trace-all $tf

Creo la topología:

- Creo los nodos:

set n1 [$ns node]

set n2 [$ns node]

set n3 [$ns node]

set n4 [$ns node]

- Creo los enlaces:

$ns duplex-link $n1 $n2 <anchoBanda><retardo><tipoCola>

$ns duplex-link $n1 $n2 1Mb 2ms DropTail

$ns duplex-link $n3 $n2 2Mb 2ms DropTail

```
$ns duplex-link $n2 $n4 2Mb 3ms DropTail
Definición de fuentes de tráfico: FTP/TCP:
set tcp [new Agent/TCP]
set tcpsink [new Agent/TCPSink]
$ns attach-agent $n3 $tcp
$ns attach-agent $n4 $tcpsink
$ns connect $tcp $tcpsink
set ftp [new Application/FTP]
$ftp attach-agent $tcp
Definición de fuentes de tráfico: CBR/UDP:
set udp [new Agent/UDP]
set null [new Agent/Null]
$ns attach-agent $n1 $udp
$ns attach-agent $n4 $null
$ns connect $udp $null
set cbr [new Application/Traficc/CBR]
$cbr attach-agent $udp
Seteo las características del tráfico CBR:
$cbr set packetSize 500 # tamaño de paquete
$cbr set interval 0.005 # tiempo entre paquetes (seg)

Defino procedimiento:
fin
proc fin {}{
global ns tf nam
puts "done!"
$ns flush-trace
close $tf
close $nam
exec nam salida.nam &
exit 0
}
```

Agendamos los eventos ycorremos el simulador:

$ns at 0.5 \$cbr start"

$ns at 1.0 "$ftp start\

$ns at 4.0 \$cbr stop"

$ns at 4.5 "$ftp stop\

$ns at 5.0 "fin"

$ns run

Características

Los agentes de tráfico se definen igual que en wired (UDP,TCP, CBR, FTP, etc, etc)

- Pueden existir nodos móviles
- Se debe definir un área en la que operarán los nodos (Topography)
- Se debe determinar las características del medio, ej: ruido
- Hay que determinar las posiciones de cada nodo
- Se debe crear un god (General Operations Director- información de la topología)

Definición de las características de los nodos Wireless

set val(chan) Channel/WirelessChannel ;# channel type

set val(prop) Propagation/TwoRayGround ;# radio-propagation model

set val(ant) Antenna/OmniAntenna ;# Antenna type

set val(ll) LL ;# Link layer type

set val(ifq) Queue/DropTail/PriQueue ;# Interface queue type

set val(ifqlen) 50 ;# max packet in ifq

set val(netif) Phy/WirelessPhy ;# network interface type

set val(mac) Mac/802 11 ;# MAC type

set val(rp) DSDV ;# ad-hoc routing protocol

Configuración de los nodos

```
$ns node - config - adhocRouting
$val(rp)
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-topoInstance $topo  \
-channel $chan  \
-agentTrace ON  \
-routerTrace ON  \
-macTrace OFF
```

Los nodos que sean creados luego dela definición anterior tendrán esas características

Con \ON" y \OFF" se elige que loguear y que no.

Ejemplo de cómo crear un nodo

```
set AP [$ns node ]
$AP random-motion 0
```

Defino la posición inicial:

```
$AP set X 5.0
$AP set Y 2.0
$AP set Z 0.0
```

Traza normal. **Fig. A38.**

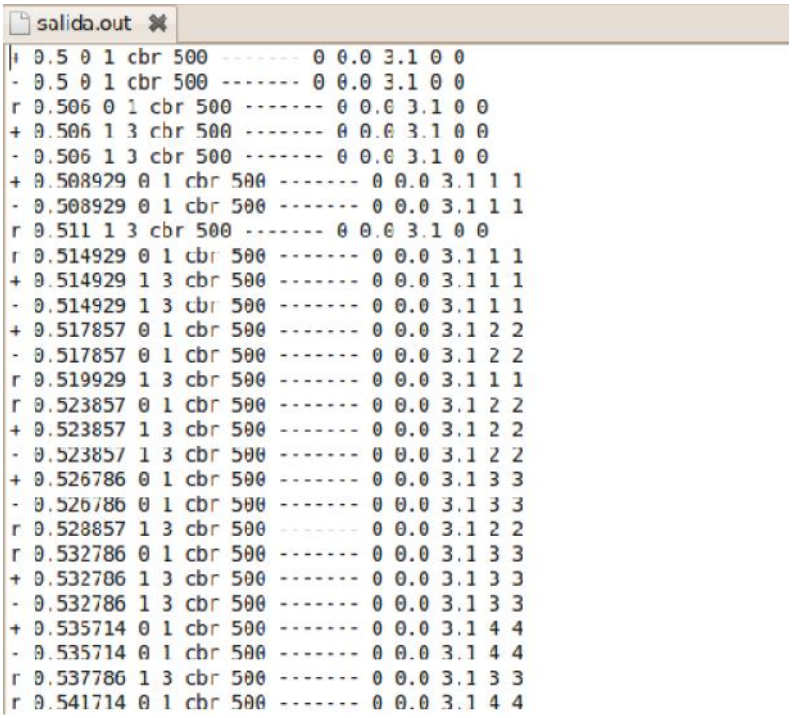


Fig. A38: Pantalla archivode salida de una Traza normal.

Traza de una simulación Wireless. **Fig. A39.**

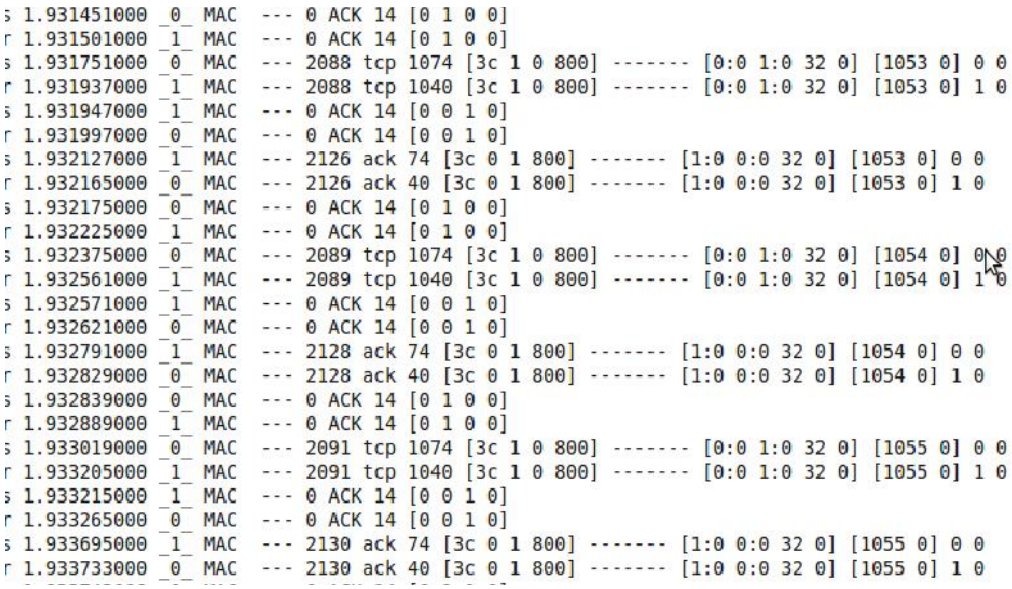


Fig. A39: Pantalla de Traza de una Simulación Wireless.