UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA

ESCUELA DE SISTEMAS

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL ENLACE POR RADIO ENTRE LA CASONA UNIVERSITARIA Y LA CASA REGIONAL DE BOLÍVAR

AUTORAS: PANATA POMA MARCIA PAZTORISA
PAZMIÑO CALERO KATTY ALEXANDRA

TUTOR: Dr. HENRY VALLEJO BALLESTEROS

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERAS EN SISTEMAS COMPUTACIONALES

Guaranda, Febrero del 2010

DEDICATORIA

Dedico esta tesis a Dios quien ha estado a mi lado en todo momento dándome las fuerzas necesarias para continuar luchando día tras día y seguir adelante rompiendo todas las barreras que se me presenten.

A mis padres ya que gracias a ellos soy quien soy hoy en día, fueron los que me dieron ese cariño y calor humano necesario, son los que han velado por mi salud, mis estudios, mi educación, a ellos a quien les debo todo, horas de consejos , de regaños, de reprimendas de tristezas y de alegrías de las cuales estoy muy seguro que las han hecho con todo el amor del mundo para formarme, a mis hermanos y hermanas los cuales me han apoyado en todo momento en especial a mi hermano Renan por haberme apoyado tanto moralmente y económicamente.

Marcia Paztorisa Panata Poma

DEDICATORIA

Tras largos años de sacrificio, dedicación y desvelos al haber culminado los estudios de Tercer Nivel, dedico con el más puro sentimiento de amor, cariño y admiración este trabajo de graduación a mi padre que está en el Cielo, a mi madre en el Oriente, a mi hijo y a mi hermana en España; quienes han sido mi fortaleza y motivación en los momentos de desesperación y tristeza, para hacerles saber que su gran anhelo se ha cumplido, aspiro cumplir con sus expectativas y nunca defraudarlos.

Katty Alexandra Pazmiño Calero

AGRADECIMIENTO

Agradecemos a Dios por habernos concedido salud y vida; por estar con nosotras en cada paso que damos, por fortalecer nuestros corazones e iluminar nuestras mentes y por habernos puesto en nuestro camino a aquellas personas que han sido nuestro soporte durante el desarrollo del proyecto de tesis hasta culminar nuestra meta de graduación.

Agradecemos hoy y siempre a nuestras familias porque a pesar de no estar presentes físicamente, sabemos que se preocuparon por nuestro bienestar, y está claro que si no fuese por el esfuerzo realizado por ellos, nuestros estudios de tercer nivel no hubiesen sido posibles.

De igual manera agradecemos a La Universidad Estatal de Bolívar, Facultad de Ciencias Administrativas Gestión Empresarial e Informática en especial a nuestra Escuela de Ingeniería en Sistemas Computacionales; También a los catedráticos quienes nos impartieron sus conocimientos y enseñanzas, en especial a nuestro Director de Tesis Dr. Henry Vallejo Ballesteros quien nos dirigió y nos motivo en cada momento a no desfallecer en nuestro objetivo.

CERTIFICADO DEL DIRECTOR

Doctor Henry Vallejo. Ms.C en mi calidad de Director de Tesis, nombrado por el H. Consejo Directivo de la Facultad de Ciencias Administrativas, Gestión Empresarial e Informática.

CERTIFICO: Que he revisado el proyecto de grado titulado " **ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL ENLACE POR RADIO ENTRE LA CASONA UNIVERSITARIA Y LA CASA REGIONAL DE BOLÍVAR".** Correspondiente periodo 2008 -2010 presentado por las Srtas. Panata Poma Marcia Paztorisa y Pazmiño Calero Katty Alexandra.

Como requisito previo para obtener el título de Ingenieras en Sistemas Computacionales.

Guaranda, 22 de febrero del 2010

Dr. Henry Vallejo. Ms.C

Director

AUTORÍA NOTARIADA

Nosotras, Marcia Paztorisa Panata Poma y Katty Alexandra Pazmiño Calero, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado para ningún grado o calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

_____ _____

Marcia Paztorisa Panata Poma Katty Alexandra Pazmiño Calero

TABLA DE CONTENIDOS

CAPITULO I

LISTA DE FIGURAS

CAPITULO I

CAPITULO II

LISTA DE CUADROS

LISTA DE ANEXOS

RESUMEN EJECUTIVO

En la matriz de la Universidad Estatal de Bolívar las Facultades y Departamentos se encuentran integradas a la red de la Universidad Estatal de Bolívar, permitiendo una fluidez de la información, ahorrando costos, tiempo y esfuerzo. Sin embargo, en la Casa Regional de Bolívar, en donde funciona el Departamento de Cultura, la Escuela de Educación y Cultura Andina de la Universidad Estatal de Bolívar, estos no se encuentran en la actualidad integradas a la red de datos de la Matriz, ya que no tienen conexión de red ni tampoco servicio de internet.

Se analizó el software a utilizarse, para lo cual nos basamos en el método inductivo que facilitó la observación, y la experimentación de los equipos y antenas permitiéndonos hacer la comparación del software del equipo que se utilizó.

Al implementar el método deductivo nos permitió una adecuada aplicación de los estándares, protocolos y todos los aspectos técnicos relacionados con el enlace de datos, demostrando que la conexión es segura y fiable.

Se implementó un enlace por radio entre la Casona Universitaria y la Casa Regional de Bolívar. La Casa Regional de Bolívar accede a los servicios que ofrece internet, además este enlace permite la conexión a la red de datos de la Universidad Estatal Bolívar.

Como un valor agregado a nuestro proyecto de graduación se brinda el servicio de internet a la comunidad universitaria a través de los Hot-Spot (Puntos de Acceso).

SUMMARIZE EXECUTIVE

In the matrix of Universidad Estatal de Bolívar all the Abilities and Departments are integrated into the net of Universidad Estatal de Bolívar, allowing a fluency of the information, saving costs, time and effort. However, in the Casa Regional de Bolívar where the Department of Culture, The School of Education and Andean Culture of Bolívar's State University works, these departments are not at the present time integrated into the net of data of the matrix, since they don't have a connection to services of the Internet.

The software will be analyzed to be used, for which we will base ourselves in the inductive method that will facilitate observation, and in turn the experimentation of the teams and the antennas will allow us to make a comparison of the software of the team with which it will be used.

The implementation of the deductive method allowed us to appropriately apply standards, protocols, and all the technical aspects related to the link of data, thereby showing that the connection is secure and reliable.

A radio link was implemented between the Casona Universitaria and the Casa Regional de Bolívar. The Casa Regional de Bolívar consents to the services that the internet offers. Moreover, this link also allows a connection to the data networking of the Universidad Estatal de Bolívar.

As an added value of our graduation project we offer internet service to the university community through the Hot-Spot (Access Points)

INTRODUCCIÓN

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder enlazar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja, está siendo ampliamente investigada en la actualidad. Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se ubican en varios pisos.

Las redes de área local inalámbricas (WLANs) constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación como: UMTS y LMDS, pues éstas requieren de un importante desembolso económico previo de parte de los operadores del servicio.

Las constantes mejoras tecnológicas y el uso de antenas direccionales, permiten que estos enlaces funcionen sobre distancias de hasta unos 40 kilómetros. Otros dispositivos comerciales proveen soluciones que permiten que los proveedores de servicios de internet (ISPs) inalámbricos proporcionen soluciones externas de punto a multipunto.

CAPITULO I

1.1 TEMA

Análisis, diseño e implementación del enlace por radio entre La Casona Universitaria y La Casa Regional De Bolívar.

1.2 ANTECEDENTES

Los tiempos están cambiando y por ende todo su alrededor, en lo social, político y cultural.

Los principales factores son los grandes avances tecnológicos que día a día se va dando para hacer la vida del hombre más cómoda; ahorrando tiempo, esfuerzo y dinero, provocando efectos de globalización sorprendentes.

Anteriormente, la comunicación implicaba mayor esfuerzo, tiempo y dinero. En la actualidad se lo hace de una manera rápida sin mucho esfuerzo y el costo ha reducido considerablemente; esto se debe al desarrollo de las telecomunicaciones, redes y nano tecnología, de las que disponemos diariamente para nuestra comodidad.

La modernización y la globalización son los principales objetivos del Estado Ecuatoriano, dadas las exigencias cada vez mayores, en los ámbitos: educativos, sociales y culturales; las Instituciones de Educación Superior están obligadas a ser las pioneras en los avances tecnológicos.

Por esta razón se efectuará el análisis del enlace de datos por radio entre La Casona Universitaria y La Casa Regional de Bolívar, logrando que los docentes, estudiantes y empleados que realizan sus actividades en esta última; se integren a la red de la Universidad, al realizar este análisis se determinará la factibilidad técnica y económica del enlace por radio, entre estos dos puntos.

1.3 PROBLEMA

En la matriz de la Universidad Estatal de Bolívar todas las Facultades y departamentos se encuentran integradas a la red de la Universidad Estatal de Bolívar, a través de fibra óptica, en otros casos cable UTP (cable par trenzado) sea categoría 5 ó 6, y en forma inalámbrica. Permitiendo una fluidez de la información, ahorrando costos, tiempo y esfuerzo.

Sin embargo, en La Casa Regional de Bolívar, en donde funcionan el departamento de Cultura, La Escuela de Cultura Andina y La Biblioteca de la Universidad, estos no se encuentran en la actualidad integrados a la red de datos de la matriz, ya que no tienen conexión de red ni tampoco servicio de internet.

1.4 JUSTIFICACIÓN

En los departamentos de la Universidad que se encuentran en La Casa Regional de Bolívar: El departamento de Cultura, La Escuela de Cultura Andina y La Biblioteca; el único medio de comunicación es a través de llamadas telefónicas, lo que implica costos elevados y pérdida de tiempo en el envío de información.

Este enlace por radio frecuencia proporcionará el acceso a la red de datos y comunicación, que beneficiará las actividades investigativas, académicas y administrativas de los departamentos en La Casa Regional de Bolívar, además se integrará a la red de datos de la Universidad, permitiéndoles tener a su disposición las herramientas tecnológicas en sus labores cotidianas. De este modo la Universidad ahorrará dinero y lo más importante, tiempo.

Nosotras, como egresadas de la Escuela de Sistemas de la Universidad Estatal de Bolívar, estamos seguras que este enlace proveerá una excelente transmisión de datos, entre La Casona Universitaria y La Casa Regional de Bolívar, al mismo tiempo se integrará esta red de datos a la matriz universitaria.

1.5 OBJETIVOS

5.1 Objetivo General

- Implementar el enlace por radio entre La Casona Universitaria y La Casa Regional de Bolívar.

5.2 Objetivos Específicos

- Analizar el funcionamiento del sistema de conexión actual a internet tanto en La Casona Universitaria como en La Casa Regional de Bolívar.
- Determinar los requisitos necesarios de hardware y software del enlace por radio para la transmisión de datos.
- Diseñar la trayectoria del enlace de datos entre La Casona Universitaria y La Casa Regional de Bolívar.
- Realizar el estudio económico.
- Monitorear la transmisión de datos del enlace por radio.
- Evaluar la transmisión de datos del enlace.

1.6 METODOLOGÍA

1.6.1 Métodos

1.6.1.1 Método Inductivo.- Es un proceso analítico sintético mediante el cual se parte del estudio de casos, hechos o fenómenos particulares para llegar al descubrimiento de un principio o ley general que los rige. Sus pasos son: Observación, experimentación, comparación, abstracción y generalización.[1]

[1] Leivazea, 1996: 17 - 18

Se analizará el software a utilizarse, para lo cual nos basaremos en el método inductivo que nos facilitará la observación, y a su vez la experimentación de los equipos y las antenas permitiéndonos hacer una comparación del software del equipo con el que se utilizará.

1.6.1.2 Método Deductivo.- Sigue un proceso sintético - analítico, es decir contrario al anterior; se presentan conceptos, principios, definiciones, leyes o normas generales de las cuales se extraen conclusiones o consecuencias en las que se aplican; o se examinan casos particulares sobre la base de las afirmaciones generales presentadas. Sus pasos son: Aplicación, compresión y demostración.[2]

Al implementar el método deductivo nos permitirá una adecuada aplicación de los estándares, protocolos y todos los aspectos técnicos relacionados con el enlace de datos, facilitándonos la demostración de los mismos.

1.6.2 Tipos de Investigación

1.6.2.1 POR EL NIVEL DEL CONOCIMIENTO

Investigación Descriptiva.- "Es la que estudia, analiza o describe la realidad presente, actual, en cuanto a hechos, personas, situaciones, etc."[3]

Por medio de la investigación descriptiva podemos analizar la situación en la que se encuentra tanto La Casona Universitaria como La Casa Regional de Bolívar, en lo que se refiere la comunicación de datos, la cual nos permitirá describir y estudiar las necesidades de dichas instancias.

[2] Leivazea, 1996: 18
[3] Leivazea, 1996: 13

Investigación Experimental.- "Es la que se refiere a lo que será, es decir, a una realidad que no existe en el momento pero que existirá después del experimento".[4]

Los departamentos de la Universidad que se encuentran laborando en La Casa Regional de Bolívar, con la implementación del enlace de datos, podrán estar comunicados y enlazados a la red de datos de la matriz universitaria.

1.6.2.2 POR LOS MEDIOS A UTILIZARSE

Investigación de Campo.- Es la que se realiza en lugares no determinados específicamente para ello; sino que corresponde al medio en donde se encuentran los sujetos o el objeto de investigación, donde ocurren los hechos o fenómenos investigados.[5]

Las pruebas tanto de los equipos como de las antenas se las realizará "in situ", lo cual nos permitirán conocer la potencia de los equipos, así como también la cobertura de las antenas, para diseñar la trayectoria del enlace de datos a través de los puntos estratégicos.

1.6.3 Técnicas e instrumentos para la obtención de datos.

1.6.3.1 Entrevista.- Es la forma verbal del cuestionario. Consiste en que un individuo proporciona directamente la información al investigador o entrevistador, en una relación que tributa a la obtención de datos, que un individuo no escribiría nunca y que difícilmente pueden ser observables.[6]

Para el análisis del funcionamiento de la red actual en La Casona Universitaria se realizará entrevistas a: Doctor Henry Vallejo, Administrador de la red; en La Casa Regional de Bolívar, al

[4] Leivazea, 1996: 14
[5] Leivazea, 1996: 13
[6] Castro, 2002: 76

Tecnólogo Antonio Tapia ayudante del museo de La Escuela de Educación y Cultura Andina y, al Doctor Rimael Núñez, Director del departamento de Cultura de la Universidad Estatal de Bolívar, para determinar sus necesidades.

1.6.3.2 Observación Directa.- La observación puede ser definida como un registro sistemático viable y confiable, que el investigador emplea para obtener directamente los datos de la realidad. Es una técnica fundamental para la recolección de datos en una investigación, aunque su uso es menor con respecto al cuestionario, quizá por no haber un dominio completo de esta técnica.[7]

Para adquirir un mayor conocimiento sobre los aspectos técnicos, relacionados a la transmisión por radio frecuencia; nos involucraremos en proyectos similares, asistiendo a conferencias y talleres.

En la determinación de los requisitos de hardware y software, se realizará una investigación a profundidad de los equipos que concuerden con las características para el enlace por radio.

En el diseño del enlace se utilizará el programa Microsoft Office Visio 2007.

El monitoreo del enlace se realizará mediante la utilización de los programas Iperf y DOS.

La evaluación del enlace se efectuará a través de los programas Microsoft Office Excel 2007, DOS.

El estudio económico se realizará mediante el análisis de los precios de los equipos y materiales necesarios para el enlace, utilizando el programa Microsoft Office Excel 2007.

[7] Castro, 2002: 73.

1.7 MARCO TEÓRICO

1.7.1 Referencial

La Universidad Estatal de Bolívar, es una entidad autónoma con personería jurídica, de derecho público, de Educación Superior. Su domicilio principal es la ciudad de Guaranda, Provincia de Bolívar. Creada mediante Ley N- 32 publicada en el registro Oficial N- 225 del 4 de julio de 1.989. Se rige por la constitución Política de la República del Ecuador, la Ley Orgánica de Educación Superior, la Ley de Creación de la Universidad Estatal de Bolívar, Estatuto, Reglamentos manuales de funciones, e instructivos y resoluciones expedidas por los organismos del sistema de educación superior establecidos en la Ley Orgánica de Educación Superior y el H. Consejo Universitario; actuando como primer Rector el Ing. Gabriel Galarza López.

La Universidad Estatal de Bolívar, cuenta con el Instituto de informática y comunicación ITIC, y con su dependencia el área de internet que provee servicios de tecnologías de la información, comunicación, investigación, desarrollo, implementación y mantenimiento de soluciones informáticas integrales para la Universidad y la comunidad.

El proyecto de investigación se realizará entre La Casa Regional de Bolívar, ubicada en las calles 7 de Mayo y Rocafuerte, y La Casona Universitaria ubicada en las calles Sucre y 10 de Agosto, frente al Parque Central de la ciudad Guaranda, Provincia Bolívar, Ecuador.

La Casona Universitaria cuenta con 29 computadoras, distribuidas de la siguiente manera: 11 computadoras en el laboratorio de computación de Post- Grado; 15 computadoras en las diferentes oficinas que laboran en La Casona Universitaria, para sus actividades diarias; 3 computadoras portátiles para los voluntarios norteamericanos del Programa World Teach.

Actualmente, existe un enlace por radio frecuencia, entre la UEB matriz y La Casona Universitaria parte del proyecto de la red inalámbrica provincial de la Universidad Estatal de Bolívar con equipos Motorola CANOPY.

En los departamentos de Cultura y La Escuela de Cultura Andina, que funciona en La Casa Regional de Bolívar, existen: 4 computadores; 2 Pentium 4 y 2 Pentium 3; también existen 2 líneas telefónicas cuyos números son: 2983-120 y 2982-013.

1.7.2 Conceptual

1.7.2.1.1. TELECOMUNICACIONES Y RED INFORMÁTICA

La especie humana es de carácter social, es decir, necesita de la comunicación; pues de otra manera viviríamos completamente aislados. Así, desde los inicios de la especie, la comunicación fue evolucionando hasta llegar a la más sofisticada tecnología, para lograr acercar espacios y tener mayor velocidad en el proceso.

Las primeras manifestaciones en la comunicación de la especie humana fueron la voz, las señales de humo y sus dibujos pictóricos; posteriormente al evolucionar, fue la escritura, el elemento que permitió desarrollar las culturas que hoy se conocen. Con el desarrollo de las civilizaciones y de las lenguas escritas surgió también la necesidad de comunicarse a distancia de forma regular, con el fin de facilitar el comercio entre las diferentes naciones e imperios.

A partir de que Benjamin Franklin demostró, en 1752, que los rayos son chispas eléctricas gigantescas, descubrimiento de la electricidad; grandes inventos fueron revolucionando este concepto, pues las grandes distancias cada vez se fueron acercando. 1836 año en que Samuel Morse creó el Telégrafo. Tomas Edison, en 1874, desarrolló la telegrafía cuádruple, la cual permitía transmitir dos mensajes simultáneamente en ambos sentidos.

A pesar de este gran avance, no era suficiente lo que lograba comunicar, es decir, esto era insuficiente pues se requería de algún medio para la comunicación de la voz. Ante esto, surge el teléfono, inventado por Alexander Graham Bell, que logra la primera transmisión de la voz en 1876.

Con los avances en el estudio de la electricidad, el físico alemán Heinrich Hertz descubre, en 1887 las ondas electromagnéticas, estableciendo las bases para la telegrafía sin hilos. Pero no fue hasta el siglo XX, cuando se inventan los tubos al vacío y el surgimiento de la electrónica, que se logran grandes avances, se inventa el radio, la primera emisión fue en 1906 en los Estados Unidos.

Desde las primeras máquinas programables manualmente (máquina diferencial de Babbage) o con procedimientos electrónicos (ENIAC, con tubos al vacío, en 1947), hasta nuestros días de potentes computadoras digitales que se han introducido en prácticamente todas las áreas de la sociedad (industria, comercio, educación, comunicación, transporte, etc.). Con todos estos avances tecnológicos y necesidades, la comunicación o transmisión de datos fue tomando cada vez más auge. Los primeros intentos y realizaciones en la tarea de conjugar ambas disciplinas - comunicaciones y procesamiento de datos - tuvieron lugar en Estados Unidos, donde durante los años cuarenta del siglo XX se desarrollo una aplicación de inventario para la U.S. Army y posteriormente, en 1953, otra para la gestión y reserva de las plazas en la American Airlines, que constituyeron los dos primeros sistemas de procesamiento de datos a distancia.

Con esta nueva necesidad y estas herramientas, surgen las redes de computadoras, las cuales son ya muy comunes en nuestros días, pero en los inicios de la transmisión por televisión y con el uso de las computadoras, la especie humana logra lanzar un vehículo espacial y tiempo después lanza los primeros satélites artificiales. Los cuales son aparatos muy sofisticados con fines múltiples (científicos, tecnológicos y militares). El primer satélite artificial, el Sputnik 1, fue lanzado por la Unión Soviética el 4 de octubre de 1957. El primer satélite de Estados Unidos fue el Explorer 1, lanzado el 31 de enero de 1958, y resultó útil para el descubrimiento de los cinturones de radiación de la Tierra.

En la actualidad hay satélites de comunicaciones, navegación, militares, meteorológicos, de estudio de recursos terrestres y científicos. La mayor parte de ellos son satélites de comunicación, utilizados para la comunicación telefónica y la transmisión de datos digitales e imágenes de televisión. Todo este desarrollo de las comunicaciones dio lugar a un nuevo concepto;

Telecomunicación que significa: Conjunto de medios de comunicación a distancia o transmisión de palabras, sonidos, imágenes o datos en forma de impulsos o señales electrónicas o electromagnéticas.

1.7.2.1.2. REDES INFORMÁTICA

Introducción

Hoy en día como todos sabemos, el futuro de nuestros países depende de la educación que se le pueda ofrecer a todo habitante de este suelo, en especial en lo tecnológico e informático los cuales, nos da diferentes tipos de soluciones eficaces y a nuestro alcance para satisfacer necesidades básicas. Ustedes se preguntarán que soluciones nos brindan las redes y seguramente se sorprenderán de lo útil que pueden llegar a ser." [8]

Hoy en día hablar de internet (la red de redes) y el uso de redes en hogares, oficinas, comercios y organismos (bancos, cybers), permite afirmar que el uso de las mismas se ha popularizado y gracias a los avances de hardware, software y la formación de estándares internacionales; utilizar una red se ha convertido en algo cotidiano y común. Las redes permiten estar conectados con el mundo, donde podemos informarnos y actualizarnos de todos los temas sobre las cuales deseamos conocer.

Definición

Conjunto de dispositivos interconectados que permiten compartir recursos e información minimizar tiempos y costos en cualquier proceso.[9]

[8] Alfonsín, 2004.
[9] Mejía, 2009.

Estos dispositivos pueden estar interconectados por un cable de red como de forma inalámbrica. Las redes fueron creadas con la idea principal de compartir información en lugares físicamente separados de una manera sencilla. Esto llevo a que se fueron agregando con el tiempo características que permitían la colaboración entre computadoras (o estaciones de trabajo) de arquitectura muy heterogénea (PCs IBM compatible, Apple Macintosh y terminales UNIX). Hoy en día esa idea original ha permanecido y ha sido potenciada por las nuevas tecnologías.[10]

1.7.2.1.3. TIPOS DE RED

Hay diferentes maneras de organizar una red y, por tanto, hay múltiples maneras de clasificarlas. Las redes pueden ser clasificadas por su ámbito geográfico, de acuerdo con su forma o topología y de acuerdo con el tipo de servicios proporcionados.[11]

a. Por su ámbito geográfico

Redes de área locales (LAN).- "Conjunto de Segmentos de red interconectados y que tienen como principal característica el acceso al medio de modo compartido".[12]

Una red de área local (LAN) abarca una distancia limitada, en general un edificio o varios próximos. La mayoría de las LAN conectan dispositivos localizados dentro de un radio de 670 metros y han sido ampliamente utilizadas para enlazar microcomputadoras. Las LAN requieren de sus propios canales de comunicaciones.[13]

Redes de área metropolitana (MAN).- "Red extendida por ciudades o provincias e interconectada por diversos medios cuya principal característica es que el acceso al medio es tanto compartido como punto a punto". Una MAN conecta diversas LAN cercanas geográficamente (en un área de

[10] Gómez, 2004.
[11] Rivera, 2009.
[12] Manizales, 2009.
[13] Rivera, 2009.

alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. Una MAN está compuesta por conmutadores o routers conectados entre sí mediante conexiones de alta velocidad (generalmente cables de fibra óptica).[14]

Red de área extensa (WAN).- "Las WAN se extienden sobrepasando las fronteras de las ciudades, provincias o naciones. Los enlaces se realizan con instalaciones de Telecomunicaciones públicas y privadas, además de enlaces por microondas y satélite".

Por costos y limitaciones técnicas una red WAN no pude tener acceso compartido, pero si una buena solución la constituye la conexión punto a punto que es la principal característica de esta red. [15]

Una de las principales características de la red WAN la constituye el uso de la red telefónica pública conmutada para el acceso al medio. La nube como es llamada es el elemento fundamental de la conexión.[16]

Red de área de almacenamiento (SAN).- Es una red de almacenamiento de cualquier tipo de información de extensión ilimitada, utilizada para preservar la información y darle confiabilidad.[17]

b. De acuerdo a su topología.

Una manera de clasificar a las redes es por su forma o topología.

TOPOLOGÍA FÍSICA

Una red informática está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos

[14] Kioska, 2008.
[15] Mora, 2009.
[16] Manizales, 2009.
[17] Manizales, 2009.

viajen correctamente). La configuración física, es decir la configuración espacial de la red, se denomina topología física.

Los diferentes tipos de topología son:

- Topología de bus
- Topología de estrella
- Topología en anillo
- Topología de árbol
- Topología de malla

La topología lógica, a diferencia de la topología física, es la manera en que los datos viajan por las líneas de comunicación. Las topologías lógicas más comunes son Ethernet y FDDI.[18]

Topología en Bus.- La red de bus enlaza a un gran número de computadoras mediante un circuito único hecho de alambre entorchado, cable coaxial o cable de fibra óptica. Todas las señales son transmitidas en ambas direcciones a toda la red, con software especial para identificar cuáles componentes reciben él mensajes; no hay una computadora central o anfitriona para controlar la red.

Fig. 1.1. Topología en Bus
Fuente: Creación Propia.

[18] Kioska, 2009.

Si una de las computadoras en la red falla, no se afecta ninguno de los otros componentes; sin embargo si se corta el medio de transmisión se cae la red. [19]

Topología en estrella.- Topología de redes en la cual todas las computadoras y los otros dispositivos están conectados a una computadora anfitriona central.

Todas las telecomunicaciones entre los dispositivos de la red deben pasar por la computadora anfitriona.

La topología es útil para aplicaciones donde algunos procesamientos deben ser centralizados y otros pueden ser realizados localmente.

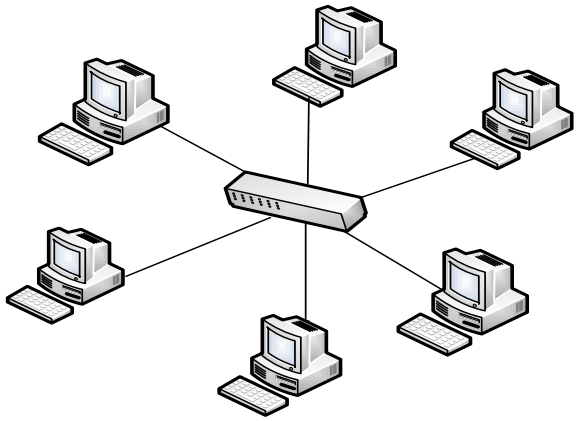


Fig. 1.2 Topología en Estrella.
Fuente: Creación Propia.

Topología en Anillo.- La red consta de una serie de repetidores (simples mecanismos que reciben y retransmiten información sin almacenarla) conectados unos a otros en forma circular (anillo). Cada estación está conectada a un repetido, que es el que pasa información de la red a la estación y de la estación a la red.

[19]Rivera, 2009.

Los datos circulan en el anillo en una sola dirección.[20]

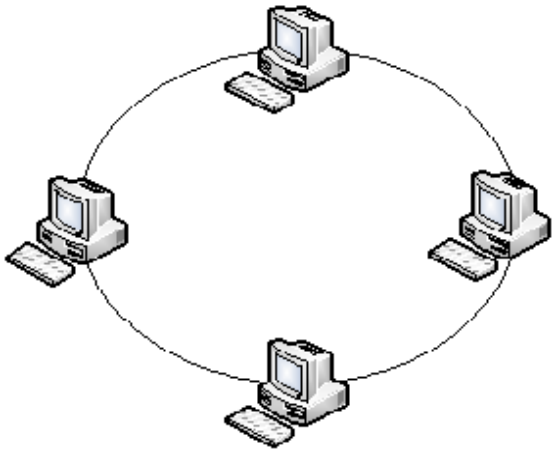


Fig. 1.3 Topología en Anillo
Fuente: Creación Propia.

Topología en árbol.- Los nodos de la red forman estrellas con la particularidad de que el centro de cada estrella. Puede conectarse a un nodo o al centro de otra estrella. En este caso, los centros de las estrellas se denominan concentradores o distribuidores

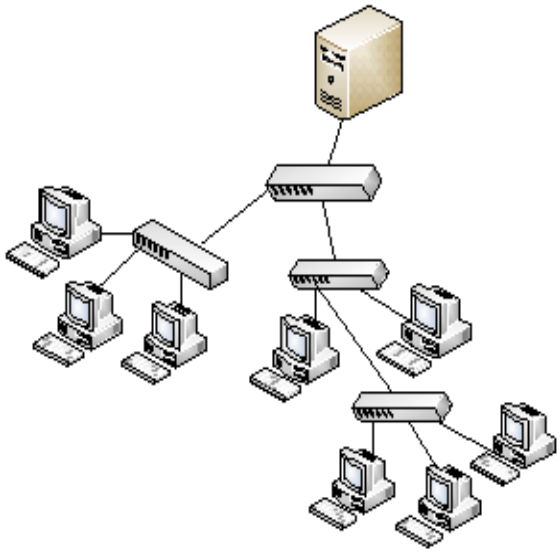


Fig. 1.4 Topología en Árbol
Fuente: Creación Propia.

[20] Cybercursos, 2009.

Topología en malla.- Muy empleada en las redes de área amplia (WAN), por su ventaja frente a problemas de tráfico y averías, debido a su multiplicidad de caminos o rutas y la posibilidad de orientar el tráfico por trayectorias opcionales.

La desventaja radica en que su implementación es cara y compleja, pero aún así, muchos usuarios la prefieren por su confiabilidad.

Internet llamada justamente la Telaraña Mundial o Red de Redes[21].

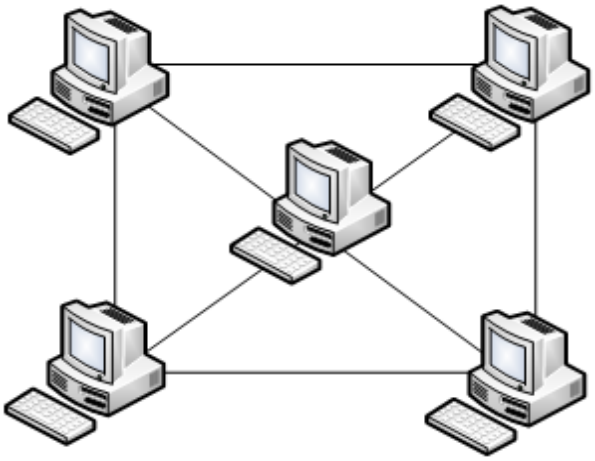


Fig. 1.5 Topología en Malla
Fuente: Creación Propia.

TOPOLOGÍA LÓGICA

ETHERNET

Estándar IEEE 802.3 es el nombre de una tecnología de redes de computadoras de área local basada en tramas de datos. El nombre viene del concepto físico de ether.

[21] Rivera, 2009.

Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.

Fig. 1.6 Topología lógica Ethernet

Fuente: Ismael Cabana, 2008.

Ethernet se refiere a las redes LAN y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama, aunque no tenga CSMA/CD como método de acceso al medio.[22]

Tramas de datos Ethernet

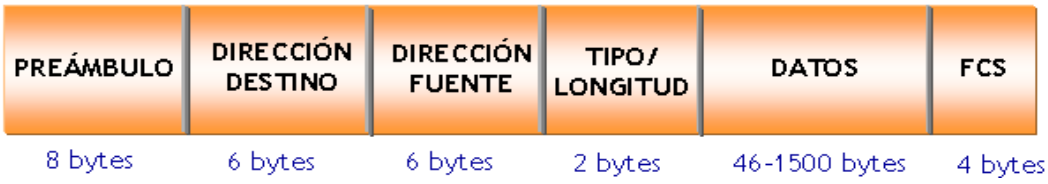


Fig. 1.7 Tramas de datos Ethernet

Fuente: Ismael Cabana, 2008.

Preámbulo.- Campo de 8 bytes que preceden al datagrama en la capa física. Tiene por finalidad permitir que las estaciones receptoras sincronicen sus

[22] Diccionario Informático, 2009.

relojes con el mensaje entrante a fin de que puedan leerlo sin errores. El último de estos bytes se denomina delimitador de comienzo de marco **SFD** ("Start Frame Delimiter").

Dirección de destino.- Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.

Dirección de origen.- Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar el paquete conoce a través de este campo la dirección de la estación origen con la cual intercambiar datos.

Tipo.- Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con el paquete, o en su defecto la longitud del campo de datos. Es interpretado en la capa de enlace de datos.

Datos.- Campo de 46 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

Secuencia de Verificación de Trama (FCS).- Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (control de redundancia cíclica). Este CRC se calcula por el emisor sobre todo el contenido de la trama, y se vuelve a calcular por el receptor para compararlo con el recibido y verificar la integridad de la trama.

TOPOLOGÍA FDDI.- La topología LAN FDDI (siglas en inglés que se traducen como interfaz de datos distribuida por fibra) es una tecnología de acceso a redes a través líneas de fibra óptica.

De hecho, son dos anillos: el anillo "primario" y el anillo "secundario", que permite capturar los errores del primero. La FDDI es una red en anillo que posee detección y corrección de errores (de ahí, la importancia del segundo anillo).

El token circula entre los equipos a velocidades muy altas. Si no llega a un equipo después de un determinado periodo de tiempo, el equipo considera que se ha producido un error en la red.

La topología de la FDDI se parece bastante al de anillo con una pequeña diferencia: un equipo que forma parte de una red FDDI también puede conectarse al hub de una MAU desde una segunda red. En este caso, obtendremos un sistema biconectado.[23]

1.7.2.1.4. MODELO OSI

El modelo de referencia OSI (Interconexión de Sistemas Abiertos), es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI.

Los fabricantes consideran que es la mejor herramienta para enseñar cómo enviar y recibir datos a través de una red. El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa.

Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red.

El modelo de referencia OSI permite visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (documentos, etc.), a través de un medio

[23] Kioskea. 2009.

de red (cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red. [24]

Estructura del Modelo OSI de ISO

Estructura multinivel.- Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación.

Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores.- Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora.

La comunicación ínter nivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

Puntos de acceso.- Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

Dependencias de Niveles.- Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados.- En cada nivel, se incorpora al mensaje un formato de control.

Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información.

Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje está constituido de dos partes: Encabezado e Información.

Unidades de información.- En cada nivel, la unidad de información tiene diferente nombre y estructura[25]

[24] Mejía, 2009.
[25] Taringa, 2009.

El modelo OSI presenta siete capas numeradas que tienen una función específica en la red. Estas son:

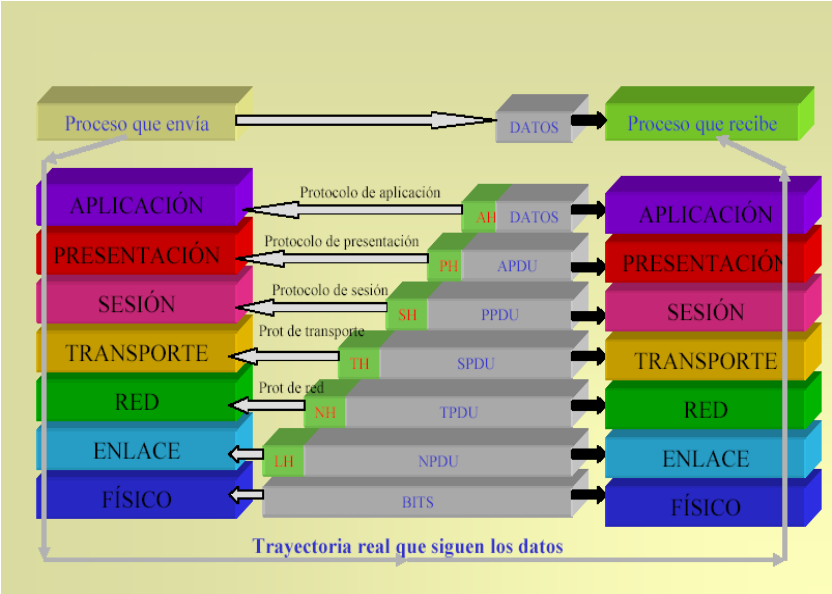


Fig. 1.8 Capas de Modelo OSI

Fuente: José Luis, 2008.

Capa física.- Es la capa que define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, ocupándose de las transmisiones a nivel de bit.

Las funciones principales de la Capa Física son:

- Permitir la compatibilidad entre los diferentes tipos de conectores existentes.
- Definir las funciones que van a realizar cada uno de los pines de los conectores.
- Establecer el tipo de cableado que se debe usar en la red.
- Determinar la codificación, el voltaje de las señales y la duración de los pulsos eléctricos.
- Coordinar la modulación de las señales, si es necesario.

- Amplificar y re temporizar las señales en su viaje a través de los medios.

Por lo tanto, incluye todos y cada uno de los elementos de red encargados de transformar los trenes de bits de las tramas en señales aptas de ser transportadas por los medios físicos y viceversa.

Los medios físicos en sí (cableado de cualquier tipo u otro medio de transmisión), los diferentes conectores de unión entre cables y dispositivos de red y los propios dispositivos que trabajan a nivel de impulsos y señales eléctricas (amplificadores, hubs y otros.). [26]

Capa de enlace de datos.- Esta capa debe de encargarse de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.[27]

El remitente parte los datos de input en marcos de datos (algunos cientos de bytes) y procesa los marcos de acuse. Este nivel maneja los marcos perdidos, dañados, o duplicados. Regula la velocidad del tráfico.

En una red de broadcast, un subnivel (el subnivel de acceso medio, o medium access sublayer*)* controla el acceso al canal compartido.

Capa de Red.- Este nivel define el enrutamiento y el envío de paquetes entre redes, es responsabilidad de esta capa establecer, mantener y terminar las conexiones.

Además proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).

[26] Mejía,2009
[27] Cybercursos,2009

Esta capa conmuta, enruta y controla la congestión de los paquetes de información en una sub-red; define el estado de los mensajes que se envían a nodos de la red. [28]

Capa de Transporte.- Acepta los datos de la capa de sesión y los divide en unidades más pequeñas si es necesario. Posteriormente los pasa a la capa de red, asegurándose que todas estas unidades lleguen correctamente al otro extremo.

En condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión.

Sin embargo, si la conexión de transporte requiere un volumen de transmisión alto, la capa de transporte podría crear múltiples conexiones (multiplexación) de red, dividiendo los datos entre las conexiones para aumentar el volumen. En cualquier caso la capa de transporte debe lograr que la multiplexación sea transparente para la capa de sesión.

Esta capa también regula el flujo de la información, a fin de que un punto de red rápido no pueda saturar uno lento. Este control de flujo, desempeña un papel muy importante, pues es la esencia del enrutamiento ordenado de paquetes.[29]

Proporciona el control de calidad del servicio (de la integridad de la información) (Ejemplo TCP/IP, IPX/SPX, NETBEUI)[30]

Capa de Sesión.- Esta capa se encarga de proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.

[28] Taringa, 2009.
[29] Mejía, 2009.
[30] García, 2009.

- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.[31]

Capa de Presentación.- La capa de presentación se ocupa de la sintaxis y la semántica de la información que se transmite.

La mayor parte de los programas de usuario no intercambian cadenas de bits al azar, sino información como nombres de personas, fechas, cantidades de dinero, por ejemplo. Estos elementos se representan con cadenas de caracteres, enteros, cantidades de punto flotante y estructuras más simples. Cada sistema puede utilizar un formato de codificación distinta (Unicode o ASCII), la capa de presentación se encarga de manejar estas estructuras y convertirlas en una representación estándar de red.[32]

Capa de Aplicación.- Proporciona servicios al usuario del Modelo OSI. Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.

Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (FTP), etc. [33]

1.7.2.1.5. MODELO DE REFERENCIA TCP

Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP Proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP).

[31] Universidad de Virginia, 1996.
[32] Mejía, 2009.
[33] Taringa, 2009.

El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, mini computadoras y computadoras centrales sobre redes de área local y área extensa.

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.[34]

El Departamento de Defensa de EE.UU. (DoD) creó el modelo TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, razón por la cual se necesitaba que la información fluyera independientemente de la condición de cualquier nodo o red en particular de la interred.

Los dos protocolos principales de TCP/IP son IP, perteneciente a la capa de red, y TCP, perteneciente a la capa de transporte. El identificador de cada puesto es la dirección IP. Una dirección IP es un número de 4 bytes. Por ejemplo: 194.142.78.95. Este número lleva codificado la dirección de red y la dirección de host. Las direcciones IP se clasifican en:

- Direcciones públicas. Son visibles desde todo Internet. Se contratan tantas como necesitemos. Son las que se asignan a los servidores de Internet que sirven información 24 horas al día (por ejemplo, un servidor web).
- Direcciones privadas. Son visibles sólo desde una red interna pero no desde Internet. Se utilizan para identificar los puestos de trabajo de las empresas. Se pueden utilizar tantas como se necesiten; no es necesario contratarlas.[35]

En la figura se muestra la comparación entre las capas del modelo OSI y el TCP, mientras en el modelo OSI se diferencian claramente siete capas, en el TCP existen solo 4 (Host a Red, Interred, Transporte y Aplicación) que agrupan varias del OSI.

[34] JuCemax, 2009.
[35] Soto, 2009.

Es común encontrar referencias donde aparecen cinco capas y otras tres, pero la más aceptada es la del modelo TCP de 4 capas.[36]

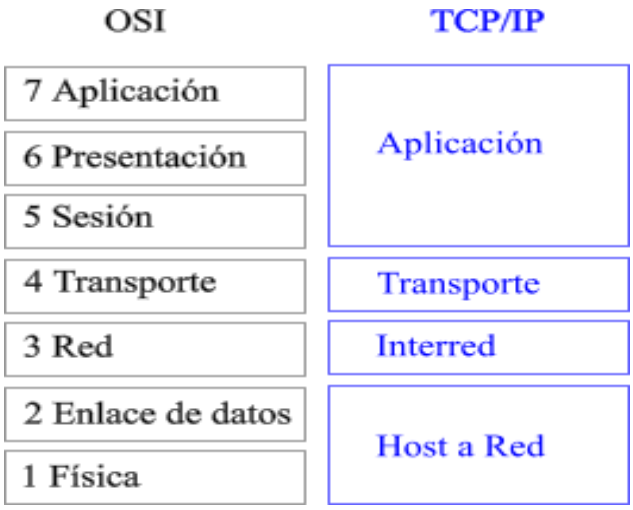


Fig. 1.9 Comparación de las Capas del modelo OSI y TCP

Fuente: Herramientas Web, 2009.

Capa de Host a Red.- El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de interred. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

Capa de Interred.- El propósito de la capa de Red es enviar paquetes origen desde cualquier red en la internetwork y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP).

En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a su destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

[36] Mejía, 2009.

En resumen el trabajo de la capa de red es entregar paquetes IP a donde se supone deben ir: Aquí la consideración más importante es claramente el enrutamiento de los paquetes, y también evitar la congestión.[37]

Capa de Transporte.- En esta capa encontramos 2 protocolos de extremo a extremo. Uno de ellos TCP (protocolo de control de la transmisión) es un protocolo confiable orientado a la conexión. El segundo protocolo de esta capa es UDP (protocolo de datagrama de usuario), es un protocolo sin conexión, no confiable, su uso es para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo.

Esta es la encargada de mantener y terminar los circuitos virtuales. Proporciona mecanismos del control de Flujo entre otras, además es la indicada para la detección y corrección de errores.

Las funciones son: fiabilidad, control de flujo, corrección de errores y retransmisión.

Capa de Aplicación.- El modelo TCP/IP no tiene capas de sesión ni presentación, aquí encontramos los protocolos de más alto nivel. El de correo electrónico SMTP, transferencia de archivos FTP, etc.

Esta capa es la más cercana a los usuarios y es la encargada de traducir los datos ya sean programas, aplicaciones para que sean envidados por la red. Las funciones que ejecuta esta capa son**:** representación, codificación, control de dialogo y gestionar las aplicaciones de usuario.[38]

1.7.2.1.6. PROTOCOLOS

Los protocolos son reglas y procedimientos para la comunicación. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos. Existen muchos protocolos a pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito

[37] Universidad de Manizales, 2009.
[38] Herramientas WEB, 2009.

diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

Algunos protocolos sólo trabajan en ciertos niveles OSI, el nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red y salgan al cable de la red.

Durante una transmisión cada protocolo se comunica con su homónimo del otro extremo sin preocuparse de los protocolos de otras capas.

Una de las decisiones más importantes que debemos tomar a la hora de diseñar una red es elegir un protocolo de la capa de acceso al medio, otro de la capa de red y transporte. La combinación más interesante para redes locales nuevas es Ethernet + TCP/IP. [39]

1.7.2.1.6.1 PROTOCOLOS DE TRANSPORTE

Facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

Intercambio de Paquetes Entre Redes (IPX/SPX)

Protocolos IPX/SPX fue desarrollada por Novell a principios de los años 80. Gozó de gran popularidad durante unos 15 años si bien actualmente ha caído en desuso. Estos protocolos fueron creados como parte del sistema operativo de red Novell NetWare.

En un principio fueron protocolos propietarios aunque más adelante se comenzaron a incorporar a otros sistemas operativos: Windows los incluye con los nombres de Protocolo compatible con IPX/SPX o Transporte compatible NWLink IPX/SPX según las versiones.[40]

[39] Axarnet, 2009.
[40] Barajas, 2009.

Definición de IPX/SPX

Los protocolos de Intercambio de paquetes entre redes (IPX) e Intercambio de paquetes secuenciados (SPX) son protocolos de transporte en redes Novel Netware. Los dos juntos corresponden al protocolo de Internet (IP) y al protocolo de control de la transmisión (TCP), utilizados en conjunto como protocolos TCP/IP.[41]

IPX/SPX es enrutable: hace posible la comunicación entre computadores pertenecientes a redes distintas interconectadas por encaminadores (routers). Los principales protocolos de IPX/SPX son, como su nombre indica, IPX y SPX.

El primero pertenece a la capa de red y se encarga del envío de los paquetes (fragmentos de mensajes) a través de las redes necesarias para llegar a su destino. SPX pertenece a la capa de transporte: gestiona el envío de mensajes completos entre los dos extremos de la comunicación.

La estructura de protocolos IPX/SPX se corresponde en gran medida con TCP/IP. Su configuración es más sencilla que en TCP/IP aunque admite menos control sobre el direccionamiento de la red. El identificador de cada puesto en la red es un número de 6 bytes, que coincide con la dirección física de su adaptador, seguido de un número de 6 bytes, que representa la dirección de la red.[42]

NetBIOS (Interfaz de Usuario Extendida para NetBIOS)

Sistema de Entrada Salida Básica de Red es un protocolo estándar de IBM, que permite que las aplicaciones sobre diferentes computadoras se comuniquen dentro de una red de área local (LAN).

NetBEUI fue creado por **IBM,** es un protocolo muy sencillo que se utiliza en redes pequeñas de menos de 10 computadores que no requieran salida a Internet. Su funcionamiento se basa en el envío de difusiones a todos los computadores de su red. Sus difusiones no atraviesan los encaminadores a no ser que estén configurados para

[41] Exa, 2009.
[42] Barajas, 2009.

dejar pasar este tráfico: es un protocolo no enrutable. La ventaja de este protocolo es su sencillez de configuración: basta con instalar el protocolo y asignar un nombre a cada computador para que comience a funcionar. Su mayor desventaja es su ineficiencia en redes grandes (se envían excesivas difusiones).

Actualmente es un protocolo exclusivo de las redes Microsoft. Fue diseñado para ofrecer una interfaz sencilla para NetBIOS (este protocolo trabaja en la capa de aplicación). NetBIOS provee los servicios de sesión descriptos en la capa 5 del modelo OSI. Es un protocolo de aplicación para compartir recursos en red. Se encarga de establecer la sesión y mantener las conexiones.

Pero este protocolo debe transportarse entre máquinas a través de otros protocolos; debido a que por sí mismo no es suficiente para transportar los datos en redes LAN como WAN, para lo cual debe usar otro mecanismo de transporte (Ej.: en redes LAN protocolo NetBEUI, en redes WAN protocolo TCP/IP). Los protocolos que pueden prestar el servicio de transporte a NetBIOS son:

- IPC/IPX
- NetBEUI
- TCP/IP [43]

Es un protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP. NetBIOS permite compartir archivos e impresoras así como ver los recursos disponibles en entorno de red.

NetBIOS utiliza los puertos 137, 138 y 139, este es exclusivo de máquinas Windows. Para averiguar si el computador tiene NetBIOS activado utilice el comando netstat - an. Este comando nos informará si tenemos los tres puertos anteriores en modo LISTENING. [44]

[43] González, 2009.
[44] Saulo, 2009.

Protocolo de Datagramas de Usuario (UDP)

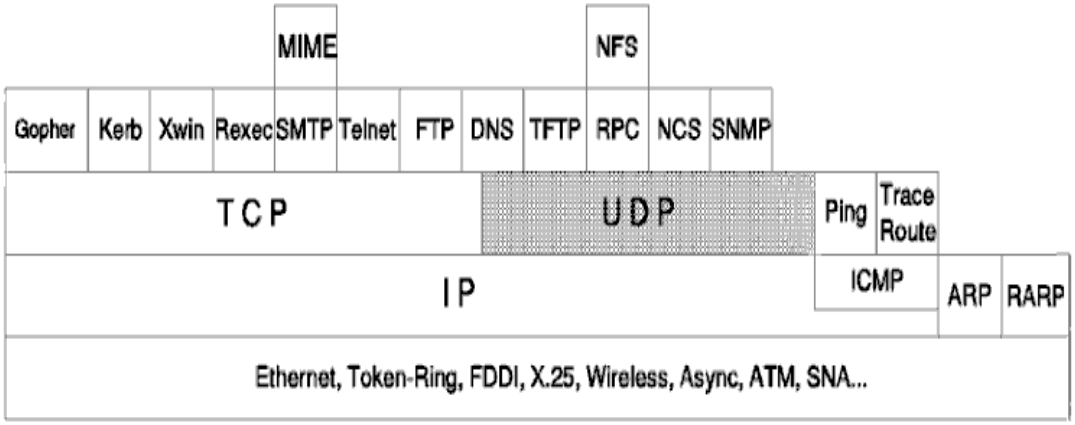


Fig. 1.10 Protocolo UDP (Protocolo de Datagramas de Usuario)

Fuente: Martín, 2009.

UDP es un protocolo estándar con número 6 de STD. Este protocolo se describe en el RFC 768 - Protocolo de Datagrama de Usuario. Este protocolo se recomienda, pero en la práctica cada implementación TCP/IP que no se use exclusivamente para encaminamiento incluirá UDP.

UDP es básicamente una interfaz de aplicación para IP. No soporta confiabilidad, control de flujo o recuperación de errores para IP. Simplemente sirve como "multiplexor/demultiplexor" para enviar y recibir datagramas, usando puertos para dirigir los datagramas como se muestra en la figura.

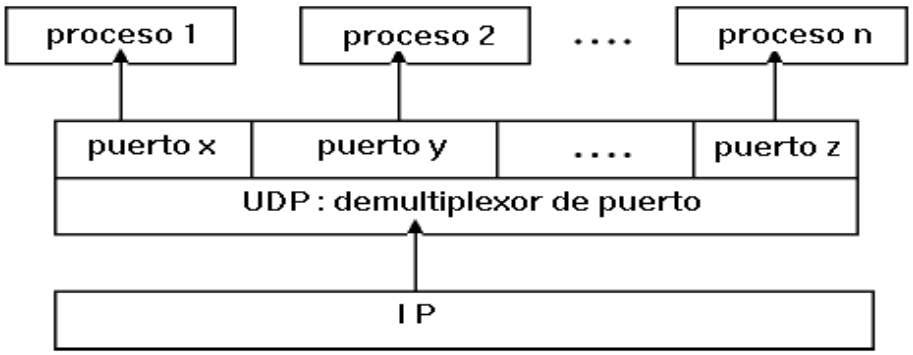


Fig. 1.11 Puertos usados por el Protocolo UDP

Fuente: Martín, 2009

UDP proporciona un mecanismo para que una aplicación envíe un datagrama a otra. La capa UDP es sumamente delgada por lo que tiene pocas sobrecargas, pero requiere que la aplicación sea responsable de la recuperación de errores y demás características no soportadas.

Puertos (Socks).- Las aplicaciones que envían datagramas hacia un host necesitan identificar el destino, siendo éste más específico que la dirección IP, ya que los datagramas están dirigidos normalmente a ciertos procesos y no al sistema completo. UDP proporciona este mecanismo usando puertos. Un puerto es un número de 16 bits que identifica qué proceso de un host está asociado con un cierto datagrama. Hay dos tipos de puerto: Bien-conocidos: Estos puertos pertenecen a servidores estándares, por ejemplo TELNET usa el puerto 23.

El rango de este tipo de puerto está comprendido entre 1 y 1023. Los números de puertos bien-conocidos son típicamente impares porque los primeros sistemas usaban el concepto de puerto como una pareja de puertos impar/par para operaciones duplex. La mayoría de los servidores requieren sólo un puerto. Una excepción es el servidor BOOTP que usa dos: el 67 y el 68.

El motivo de la utilización de los puertos bien-conocidos es permitir a los clientes tener la capacidad de encontrar servidores sin información de configuración. Los números de dichos puertos están definidos en STD 2 - números de internet asignados.

Efímeros: Los clientes no necesitan números de puertos bien-conocidos porque inician la comunicación con servidores y el número de puerto que usan ya está contenido en los datagramas UDP enviados al servidor. Cada proceso del cliente está localizado en un número de puerto mientras el host lo necesite y se esté ejecutando. Los números de puerto efímeros tienen valores mayores que 1023, normalmente en el rango de 1024 a 5000. Un cliente puede usar cualquier número localizado dentro de dicho rango, mientras que la combinación de <protocolo de transporte, dirección IP, número de puerto> es única.

Nota: TCP también usa números de puerto con los mismos valores. Estos puertos son bastante independientes. Normalmente, un servidor usará TCP o UDP, pero hay excepciones. Por ejemplo, los servidores de Nombres de Dominio usan ambos, puerto UDP 53 y puerto TCP 53.

Formato del Datagrama UDP

Cada datagrama UDP se envía con un único datagrama IP. Aunque el datagrama IP se puede fragmentar durante la transmisión, la implementación de recepción IP lo re-ensamblará antes de presentarlo a la capa UDP. Todas las implementaciones IP están preparadas para aceptar datagramas de 576 bytes, permitiendo un tamaño máximo de cabecera IP de 60 bytes sabiendo que un datagrama UDP de 516 bytes lo aceptan todas las implementaciones. Muchas implementaciones aceptarán datagramas mayores, aunque no se puede asegurar. El datagrama UDP tiene una cabecera de 16 bytes que se describe en la figura.

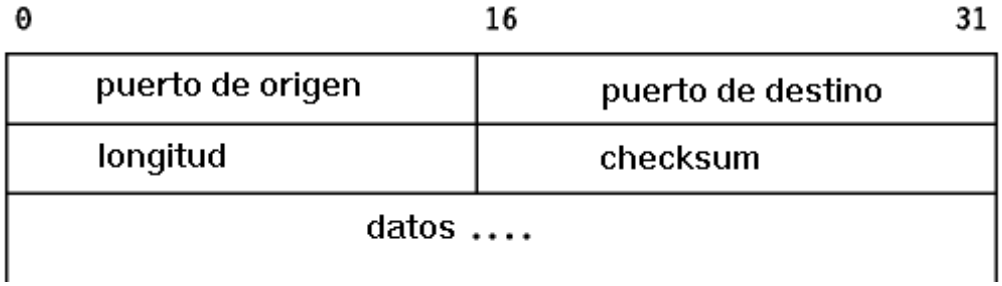


Fig. 1.12 Formato del Datagrama UDP

Fuente: Martín, 2009

Donde:

Puerto de origen.- Indica el puerto del proceso que envía. Este es el puerto que se direcciona en las respuestas.

Puerto destino.- Específica el puerto del proceso destino en el host de destino.

Longitud.- Es el tamaño (en bytes) de este datagrama de usuario incluyendo la cabecera.

Suma de comprobación (checksum).- Es un campo opcional de 16 bits en complemento a uno de la suma en complemento a uno de una cabecera pseudo-IP, la cabecera UDP y los datos UDP. La cabecera pseudo-IP contiene la dirección IP fuente y destino, el protocolo y la longitud UDP:

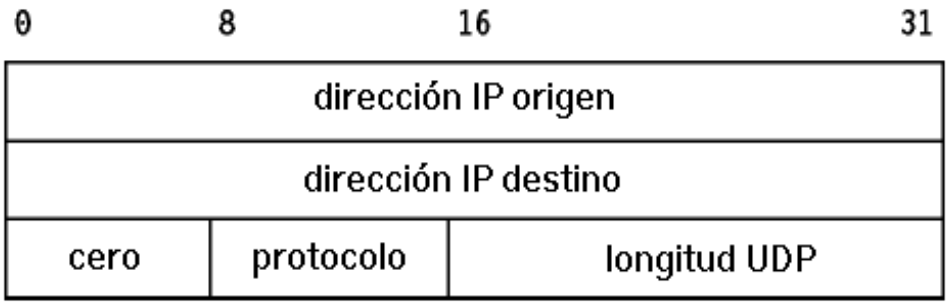


Fig. 1.13 Suma de comprobación
Fuente: Martín, 2009

La cabecera pseudo-IP extiende efectivamente la suma de comprobación para incluir el datagrama IP original (defragmentado).

Las aplicaciones estándares que utilizan UDP son:

- Protocolo de Transferencia de Ficheros Trivial (TFTP)
- Sistema de Nombres de Dominio (DNS) servidor de nombres
- Llamada a Procedimiento Remoto (RPC), usado por el Sistema de Ficheros en Red (NFS)
- Sistema de Computación de Redes (NCS)
- Protocolo de Gestión Simple de Redes (SNMP) [45]

[45] Martín, 2009.

TCP (Protocolo de Control de Transmisión)

TCP es un protocolo estándar con el STD 7. Se describe en el RFC 793 – TCP ("Transmission Control Protocol"). Su status es recomendado, pero en la práctica cualquier implementación de TCP/IP que no se use exclusivamente para el encaminamiento incluirá TCP.

TCP proporciona una cantidad mayor de servicios a las aplicaciones que UDP, notablemente, la recuperación de errores, control de flujo y fiabilidad. Se trata de un protocolo orientado a conexión a diferencia de UDP. La mayoría de los protocolo de aplicación de usuario, como TELNET y FTP, usan TCP.

TCP usa el mismo principio de puerto que UDP, para conseguir multiplexación. Al igual que UDP, TCP utiliza puertos efímeros y bien conocidos. Cada extremo de una conexión TCP tiene un zócalo que puede identificarse con la tripleta <TCP, dirección IP address, número de puerto>.

Fig. 1.14 TCP (Transmission Control Protocol)
Fuente: Universidad de Murcia, Facultad de Informática.

Es lo que se llama un medio asociado. Si dos procesos se están comunicando sobre TCP, tendrán una conexión lógica identificable unívocamente por medio de los dos zócalos implicados, es decir, con la combinación <TCP, dirección IP local, puerto

local, dirección IP remota, puerto remoto>. Los procesos del servidor son capaces de gestionar múltiples conversaciones a través de un único puerto.

Fig. 1.15 Conexión TCP - Los procesos X e Y se comunican sobre una conexión TCP que emplea datagramas IP

Fuente: Universidad de Murcia, Facultad de Informática, 2009

El principal propósito de TCP es proporcionar una conexión lógica fiable entre parejas, procesos. No asume la fiabilidad de los protocolos de niveles inferiores (como IP) por lo que debe ocuparse de garantizarla.

TCP se puede caracterizar por los siguientes servicios que suministra a las aplicaciones que lo usan:

- **Transferencia de datos a través de un canal.-** Desde el punto de vista de la aplicación, TCP transfiere un flujo continuo de bytes a través de internet. La aplicación no ha de preocuparse de trocear los datos en bloques o en datagramas. TCP se encarga de esto al agrupar los bytes en segmentos TCP, que se pasan a IP para ser retransmitidos al destino. Además, TCP decide por sí mismo cómo segmentar los datos y puede enviarlos del modo que más le convenga.

  A veces, una aplicación necesita estar segura de que todos los datos pasados a TCP han sido transmitidos efectivamente al destino. Por esa razón, se

define la función "push". Esta función mandará todos los segmentos que sigan almacenados al host de destino. El cierre normal de la conexión también provoca que se llame a esta función, para evitar que la transmisión quede incompleta.

- **Fiabilidad.-** TCP asigna un número de secuencia a cada byte transmitido, y espera un reconocimiento afirmativo (ACK) del TCP receptor. Si el ACK no se recibe dentro de un intervalo de timeout, los datos se retransmiten. Como los datos se transmiten en bloques (segmentos de TCP), al host de destino sólo se le envía el número de secuencia del byte de cada segmento.

  El TCP receptor utiliza los números de secuencia para organizar los segmentos cuando llegan fuera de orden, así como para eliminar segmentos duplicados.

- **Control de flujo.-** El TCP receptor, al enviar un ACK al emisor, indica también el número de bytes que puede recibir aún, sin que se produzca sobrecarga y desbordamiento de sus buffers internos. Este valor se envía en el ACK en la forma del número de secuencia más elevado que se puede recibir sin problemas. Este mecanismo se conoce también como mecanismo de ventanas.

- **Multiplexación.-** Se consigue usando puertos, al igual que en UDP.

- **Conexiones lógicas.-** La fiabilidad y el control de flujo descritos más arriba requieren que TCP inicialice y mantenga cierta información de estado para cada canal. La combinación de este estado, incluyendo zócalos, números de secuencia y tamaños de ventanas, se denomina conexión lógica. Cada conexión se identifica unívocamente por el par de zócalos del emisor y el receptor.

- **Full Duplex.-** TCP garantiza la concurrencia de los flujos de datos en ambos sentidos en la conexión.

Un simple protocolo de transporte podría emplear el siguiente principio: enviar un paquete, y esperar un reconocimiento del receptor antes de enviar el siguiente. Si el ACK no se recibe dentro de cierto límite de tiempo, se retransmite.

Fig. 1.16 El principio de la ventana
Fuente: Universidad de Murcia, Facultad de Informática, 2009

Aunque este mecanismo asegura fiabilidad, sólo usa una parte del ancho de banda de la red que está disponible. Considerar ahora un protocolo en el que el emisor agrupa los paquetes que va a transmitir.

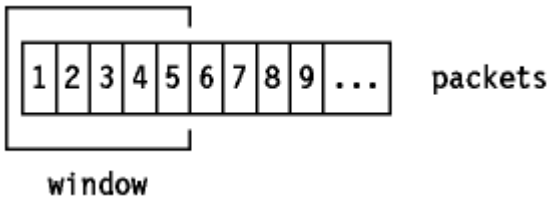


Fig. 1.17 Paquetes del mensaje
Fuente: Universidad de Murcia, Facultad de Informática, 2009

Y utiliza las siguientes reglas:

- El emisor puede enviar todos los paquetes dentro de la ventana sin recibir un ACK, pero debe disparar un cronómetro para el timeout para cada uno de ellos.

- El receptor debe reconocer cada paquete recibido, indicando el número de secuencia del último paquete bien recibido.
- El emisor desliza la ventana para cada ACK recibido.

En nuestro ejemplo, el emisor puede transmitir paquetes del 1 al 5 sin esperar respuesta:

Fig. 1.18. El principio de la ventana
Fuente: Universidad de Murcia, Facultad de Informática, 2009

En el momento en que el emisor recibe el ACK 1, puede deslizar su ventana para excluir el paquete 1: En este punto, el emisor puede transmitir también el paquete 6.

Fig. 1.19 Paquetes del mensaje
Fuente: Universidad de Murcia, Facultad de Informática, 2009

Imaginar algunos casos especiales:

- El paquete 2 se pierde: el emisor no recibirá ACK 2, por lo que su ventana permanecerá en posición 1(como se ve en el último dibujo). De hecho, como el receptor no recibió el paquete 2, reconocerá los paquetes 3, 4 y 5 con un ACK 1, que fueron los últimos paquetes recibidos en secuencia. En el extremo del emisor, al final se producirá un timeout para el paquete 2 y se

retransmitirá. Notar que la recepción de este paquete en el receptor generará un ACK 5, ya que se habrán recibido con éxito los paquetes del 1 al 5, y la ventana del emisor se deslizará cuatro posiciones al recibir el ACK 5.

- El paquete 2 llegó, pero el reconocimiento se perdió: el emisor no recibe ACK 2, pero recibe ACK 3. ACK 3 es un reconocimiento de todos los paquetes hasta el 3(incluyendo el 2) y el emisor ya puede deslizar su ventana hasta el paquete 4.

Este mecanismo de ventanas asegura:

- Transmisión fiable
- Mejor aprovechamiento del ancho de banda (mejora del flujo).
- Control de flujo, ya que el receptor puede retrasar la respuesta a un paquete con un reconocimiento, conociendo los buffers libres de los que dispone y el tamaño de la ventana de comunicación. [46]

INTERNET

Es una red de redes de millones de computadores en todo el mundo, pero al contrario de lo que se piensa comúnmente, internet no es sinónimo de World Wide Web. La Web es sólo una parte de internet, es sólo uno de los muchos servicios que ofrece internet.

Internet suministra un foro de comunicación en el que participan millones de personas de todos los países del mundo, en mayor o menor medida. Internet aporta o soporta una serie de instrumentos para que la gente difunda y acceda a documentos y a la información (WWW, FTP, etc.), para que los individuos y los grupos se relacionen a través de una serie de medios de comunicación más o menos nuevos (correo electrónico, news, listas de distribución, videoconferencia, chats...) o más o menos viejos (como una conversación telefónica, poner un fax, etc.,) y también incluye dentro de sí a los denominados medios de comunicación

[46] Tutorial TCP/IP, 2009.

de masas (radio, televisión, periódicos y revistas "on line", cine, la omnipresente publicidad, etc.). ¿Se trata de un nuevo medio de comunicación? ¿Pueden utilizarse las nociones habituales que se aplican a los medios de comunicación para definir y caracterizar la comunicación en internet?

En realidad, internet no es un medio de comunicación, sino muchos medios, una red que comprende distintos tipos y distintos sistemas de comunicación. La gente utiliza internet para distintas finalidades. Muchas de ellas están relacionadas con diferentes y variadas categorías de comunicación, información e interacción.

Sin embargo, internet no configura una nueva sociedad, sino que forma parte de ella, aunque se produzca y reproduzca al otro lado de las redes. Esos dos espacios, el de fuera y el de dentro de las redes, están indisolublemente entrelazados y se transforman mutuamente. Los interactores son las mismas personas y los mismos agentes sociales a uno y otro lado de las pantallas, de las redes y las tecnológicas.

El nacimiento de la galaxia internet ha dado origen a numerosos estudios y publicaciones sobre las repercusiones de este nuevo espacio social de interacción y sus implicaciones sobre el arte, la cultura, la ciencia, la ecología, la economía, los medios de información y comunicación, el mundo laboral, la empresa, la política y cada una de las actividades humanas.[47]

Servicios de Internet

Los servicios disponibles en internet aparte de la Web, son el acceso remoto a otros computadores (a través de telnet o siguiendo el modelo cliente/servidor), la transferencia de ficheros (FTP), el correo electrónico (e-mail), los boletines electrónicos y grupos de noticias, las listas de distribución, los foros de debate y las conversaciones en línea (chats).

En internet también se puede escuchar la radio, ver la televisión, asistir a un concierto, visitar un museo o jugar a través de la red.

[47] Barnes, 2009.

Las actividades diarias realizadas en internet son las siguientes: [48]

ACTIVIDADES DIARIAS ONLINE		
ACTIVIDAD	% de aquellos con acceso a Internet	Fecha del dato
Enviar correo	52	Marzo-mayo 2008
Obtener noticias	32	Marzo-mayo 2008
Usar un buscador para obtener información	29	Enero 2008
Navegar por la Web para divertirse	23	marzo-mayo 2008
Buscar información sobre algún hobby	21	marzo-mayo 2008
Hacer una búsqueda en Internet para responder a una cuestión específica	19	septiembre 2008
Hacer algún tipo de comprobación para el trabajo	19	noviembre 2008
Comprobar un producto o servicio antes de comprarlo	19	diciembre 2008
Consultar el tiempo	17	marzo-mayo 2007
Enviar un mensaje instantáneo	14	marzo-mayo 2007

Cuadro. 1.1 Actividades Online

Fuente: María Jesús Lamarca Lapuente, 2009.

Correo Electrónico

Es un servicio de internet que permite enviar y recibir mensajes entre emisor y receptor cuando estos han acordado el intercambio. Es uno de los servicios más utilizados debido a que facilita las comunicaciones en cualquier momento y a cualquier parte. Se basa en el protocolo TCP/IP y su esquema de conexión es asíncrono, es decir, no requiere establecer una conexión entre emisor y receptor para transmitir.

[48] PIALP, 2009.

Por lo tanto al enviar un mensaje se requiere que el receptor revise su correo electrónico para leerlo, de lo contrario este permanece almacenado en un servidor de correo hasta que el usuario lo busque. Es un error pensar que en el correo electrónico el receptor conocerá el mensaje inmediatamente después de enviado, para esto se requiere una conexión sincrónica o en línea, donde tanto trasmisor como receptor están listos para iniciar la charla, ejemplo de una comunicación de este estilo es el servicio de Chat.

El Funcionamiento del correo electrónico.- El correo electrónico utiliza el protocolo de comunicación SMTP (Simple Mail Transfer Protocol), este protocolo es el encargado de establecer la comunicación entre servidores de correo. Una vez establecida, el servidor de correo que recibe el mensaje lo almacena en los buzones de correo de los usuarios.

Posteriormente el usuario con la ayuda de un cliente de correo busca los mensajes que están en su correo, en este momento se pueden usar dos tipos de protocolos de comunicación, el POP3 y el IMAP, la diferencia entre estos está en la forma como descargan los correos del buzón del servidor al buzón del cliente o bandeja de entrada, mientras el POP3 descarga el mensaje totalmente, el IMAP lo hace por partes.[49]

WEB

WWW son las iniciales de World Wide Web, el sistema de documentos de hipertexto que se encuentran enlazados entre sí y que son accesibles a través de Internet. Mediante un software conocido como navegador, los usuarios pueden visualizar las páginas web (que contienen texto, imágenes, videos y otros contenidos multimedia) y navegar a través de ellas mediante los hipervínculos.

[49] Caribdis, 2009.

La WWW fue desarrollada a inicios de la década de los 90 por el inglés Tim Berners-Lee y el belga Robert Cailliau, mientras trabajaban en el CERN de Ginebra (Suiza). De todas formas, sus antecedentes se remontan a los años 40. Hay que destacar que Berners-Lee y Cailliau han sido claves para la creación de los estándares web, como los lenguajes de marcado con los que se crean las páginas.

El funcionamiento de la WWW comienza cuando un usuario ingresa una dirección (URL) en su navegador o cuando sigue un enlace de hipertexto presente en una página. El navegador entonces inicia una serie de comunicaciones para obtener los datos de la página solicitada y, de esta forma, visualizarla.

El primer paso consiste en transformar el nombre del servidor de la URL en una dirección IP, utilizando la base de datos conocida como DNS. La dirección IP permite contactar al servidor web y enviarle los paquetes de datos.

Luego se envía una petición HTTP al servidor, solicitando el acceso al recurso. Primero se solicita el texto HTML y después es analizado por el navegador, que realiza peticiones adicionales para los gráficos y otros archivos que formen parte de la página.[50]

El Chat

Es un sistema mediante el cual dos o más personas pueden comunicarse a través de Internet, en forma simultánea, es decir en tiempo real, por medio de texto, audio y hasta video, sin importar si se encuentra en diferentes ciudades o países.

[50] Maringa, 2009.

Puede entablar comunicación con amigos, familiares, compañeros de trabajo e incluso con gente desconocida, sólo tiene que elegir la sala y checar que la persona esté en línea. Es un medio muy económico porque te puedes comunicar a cualquier parte del mundo y no tienes que pagar llamadas de larga distancia.

Un chat está conformado por una o varias salas o canales, los cuales son cuartos virtuales en donde la gente se reúne para comunicarse e intercambiar ideas sobre un tema en particular, o puedes platicar en privado con personas conocidas o desconocidas. Estos clubes están clasificados por temas como salud, romance, medicina, música, cine, cultura, etc.

Técnicamente podemos decir que los chat room son lugares virtuales que se encuentran en un servidor de internet el cual administra todos los mensajes, tanto los que mandas como los que recibes.[51]

Videoconferencia

Es una tecnología que proporciona un sistema de comunicación bidireccional de audio, video y datos que permite que las sedes receptoras y emisoras mantengan una comunicación simultánea interactiva en tiempo real.

Se requiere utilizar equipo especializado que te permita realizar una conexión a cualquier parte del mundo sin la necesidad de trasladarse al un punto de reunión. La videoconferencia involucra la preparación de la señal digital, la transmisión digital y el proceso de la señal que se recibe. Cuando la señal es digitalizada esta se transmite vía terrestre o por satélite a grandes velocidades.

[51] Ciberhabitat, 2008.

Para que la videoconferencia se realice se debe de comprimir la imagen mediante un CODEC. Los datos se comprimen en el equipo de origen, viajan comprimidos a través de algún circuito de comunicación, ya sea terrestre o por satélite y se descomprime en el lugar de destino. [52]

Aplicaciones.- Hoy en día la videoconferencia es una parte muy importante de las comunicaciones es por esa razón que día a día se va descubriendo nuevas aplicaciones dentro de la educación tenemos:

- Educación a distancia
- Investigación y vinculación
- Reuniones de academia
- Formación continua
- Reunión ejecutiva
- Congresos
- Conferencias
- Cursos
- Seminarios
- Otros

A quién beneficia.- La videoconferencia se ha vuelto una tecnología que se ha colocado al alcance de todos principalmente a brindar servicios a:

Alumnos

- Permite recibir una educación de altísimo nivel con oportunidades de capacitación solamente disponibles en institutos de primera.
- Tener a su disposición técnicas avanzadas en los campos educacionales.
- Recibir conocimientos impartidos por eminencias en cada tema.

[52] STE DGSCA UNAM, 2009.

- Tener la posibilidad de realizar cualquier pregunta a los conferencistas, con el fin de obtener las mejores respuestas a sus dudas.
- Asistir a las conferencias sin necesidad de abandonar el campus educacional.

Académicos

- Permite impartir cátedra a distancia
- Mantener una comunicación cara a cara con los estudiantes sin tener la necesidad de trasladarse a un aula de clases.
- Asistir a conferencias sin la necesidad de abandonar el campus.

Investigadores

- Asistir a eventos importantes sin la necesidad de trasladarse al lugar sede.
- Comunicarse con colegas cara a cara para poder intercambiar puntos de vista.
- Impartir conferencias a distintas partes del mundo desde una sede.

Funcionarios

- Asistir a eventos sin la necesidad de trasladarse
- Poder comunicarse con su personal sin la necesidad de estar presente.
- Mantener una comunicación cara a cara con otros funcionario[53]

VoIP (Voz Sobre IP)

Es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La telefonía IP es una aplicación

[53]RIV UAEH, 2009.

inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares.

En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportada vía redes IP, internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

En general, esto quiere decir enviar voz en forma digital en paquetes en lugar de enviarla en forma de switcheo de circuitos como una compañía telefónica convencional.

La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) por las compañías ordinarias. En la actualidad la calidad de voz es indistinta entre una llamada Bois o una llamada convencional.[54]

Funcionamiento de la Telefonía IP

Los pasos básicos que tienen lugar en una llamada a través de internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

Cuando se hace una llamada telefónica por IP, nuestra voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de internet a la persona con la que estamos hablando. Cuando alcanzan su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

[54] Tsares, 2009.

Hay tres tipos de llamadas:

- PC a PC, siempre gratis.
- PC a Teléfono, gratis en algunas ocasiones, depende del destino.
- Teléfono a Teléfono, muy baratas.

¿En qué se diferencia la Telefonía IP de la telefonía normal?

En una llamada telefónica normal, la central telefónica establece una conexión permanente entre ambos interlocutores, conexión que se utiliza para llevar las señales de voz. En una llamada telefónica por IP, los paquetes de datos, que contienen la señal de voz digitalizada y comprimida, se envían a través de internet a la dirección IP del destinatario. Cada paquete puede utilizar un camino para llegar, están compartiendo un medio, una red de datos. Cuando llegan a su destino son ordenados y convertidos de nuevo en señal de voz.[55]

Gopher

Permite buscar recursos utilizando menús. Cuando encuentra algo que le gusta puede leerlo o tener acceso a ello a través de gopher sin necesidad de preocuparse por los nombres de dominio, los domicilios IP o por cambiar de programas. Gopher es un potente sistema que permite acceder a muchos de los recursos de INTERNET de una forma simple y consistente. Para usar Gopher, todo lo que se necesita es seleccionar en un menú.

La potencia de Gopher viene de que los recursos numerados en un menú pueden estar en cualquier parte de internet. Cuando se selecciona un elemento, Gopher lo traerá o hará lo que sea necesario para atender nuestra petición. La mayor parte del tiempo, Gopher tendrá que conectarse a otra computadora, pero todo será transparente. Todo lo que notaremos es que nuestra petición ha sido cumplida simple y fácilmente.

[55] Ocitel, 2009.

La ventaja que ofrece el Gopher no es tanto que ahorre la búsqueda de direcciones o nombres de recursos, o que no se tenga necesidad de utilizar varios comandos para obtener lo que se desea. La ventaja real consiste en que permite curiosear a través de los recursos de internet, sin importar su tipo, tal como si se hojeara el catálogo de la biblioteca local que contiene libros, imágenes y registros sonoros, todo agrupado en un solo volumen.

Cómo Funciona Gopher

Gopher es un sistema cliente-servidor. Para usar Gopher, hay que ejecutar un programa llamado Cliente Gopher. De vez en cuando el cliente gopher contacta con un servidor gopher para pedirle información en nuestro nombre. Si fuera necesario contactar con otro tipo de servicio, digamos, abrir una sesión telnet o cargar un archivo, el cliente gopher también se cuidará de eso.

Requerimientos

Para tener acceso al sistema Gopher, se necesita un programa cliente gopher. El programa cliente especial debe estar instalado en una computadora que se encuentre en internet.

Algunos ejemplos de la información que gopher puede ofrecer:

- Pronósticos y mapas del tiempo
- Recetas
- Problemas y respuestas de temas de computación
- Acceso a news
- Libros de los clásicos, de Shakespeare, Moby Dick, etc.
- Catálogos de bibliotecas de todo el mundo
- Catálogos de cursos universitarios [56]

[56] Lyco, 2009.

Telnet

Es un protocolo de internet estándar que permite conectar terminales y aplicaciones en internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma Terminal virtual de red (NVT);
- El principio de opciones negociadas;
- Las reglas de negociación.

Éste es un protocolo base, al que se le aplican otros protocolos del conjunto TCP/IP (FTP, SMTP, POP3, etc.). Las especificaciones Telnet no mencionan la autenticación porque Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet).

Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada). Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.[57]

[57] Álvarez, 2009.

Telnet es un servicio típico que viene con los servidores dedicados. Como un servidor dedicado sólo lo utiliza un único usuario, con telnet se puede configurar a su gusto cualquier cosa del servidor. A través de telnet nos resulta muy cómodo realizar algunas acciones de administración, como backups, migraciones, planificación automática de tareas periódicas, reparación del servidor ante caídas, etc.

Existe diversos programas cliente que podemos utilizar para hacer telnet. Uno muy popular es Putty. [58]

Protocolo de Transferencia de Ficheros (FTP)

Es la herramienta que permite a través de la red copiar ficheros de un computador a otro, sin importar en absoluto donde están localizados estos computadores, ni si usan o no el mismo sistema operativo: basta con que estén conectados a internet.

El programa permite manipular toda clase de ficheros, tanto si son tipo texto como si son ejecutables, independientemente de que estos se hallen comprimidos o empaquetados. Tampoco tiene importancia el sistema operativo en que han sido almacenados o al que van destinados; ya sea DOS, UNIX, Windows, Macintosh o cualquier otro.

La finalidad de este programa, es facilitar la copia o el traslado de ficheros desde el disco de un computador al disco de otro, sin correr ningún tipo de riesgo de pérdida de información; y de una manera rápida y a la vez muy sencilla.

Normalmente, un usuario utilizará un programa cliente FTP para acceder a un servidor en el que estará funcionando un servidor FTP. Los programas servidores FTP no suelen encontrarse corrientemente en los

[58] Pillou, 2009.

computadores personales, por lo que un usuario normalmente utilizará el FTP para traerse ficheros de servidor FTP anónimo o para depositar ficheros en un servidor para su almacenamiento, su publicación como páginas WWW, etc.

Para acceder a un FTP anónimo sólo para ver y traer ficheros, puede utilizar también un navegador de internet (NetScape, MS-Explorer, etc), estos programas también son clientes FTP de sólo lectura. Se reservan los servidores HTTP (de páginas WEB) para depositar información tipo textual, principalmente destinada a la lectura interactiva.[59]

1.7.2.1.6.2 PROTOCOLOS DE RED

Proporcionan lo que se denominan servicios de enlace. Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

Protocolo Internet (IP)

Es un protocolo de internetworking que provee servicios, sin conexión, a través de múltiples redes de conmutación de paquetes. La versión vigente, durante décadas, ha sido IPv4**.**

Intercambio de Paquetes Internet (IPX)

Protocolo de Comunicaciones de NetWare, utilizado para enrutar mensajes de un nodo a otro. Los paquetes IPX incluyen las direcciones de red. IPX no asegura que los mensajes enrutados lleguen a su destino, por lo que se requiere que la aplicación provea de esa seguridad, o que se utilice el protocolo SPX.

[59] Álvarez, 2009.

NetBEUI

Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.[60]

Protocolo de Mensajes de Control y Error (ICMP)

Se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

Únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:

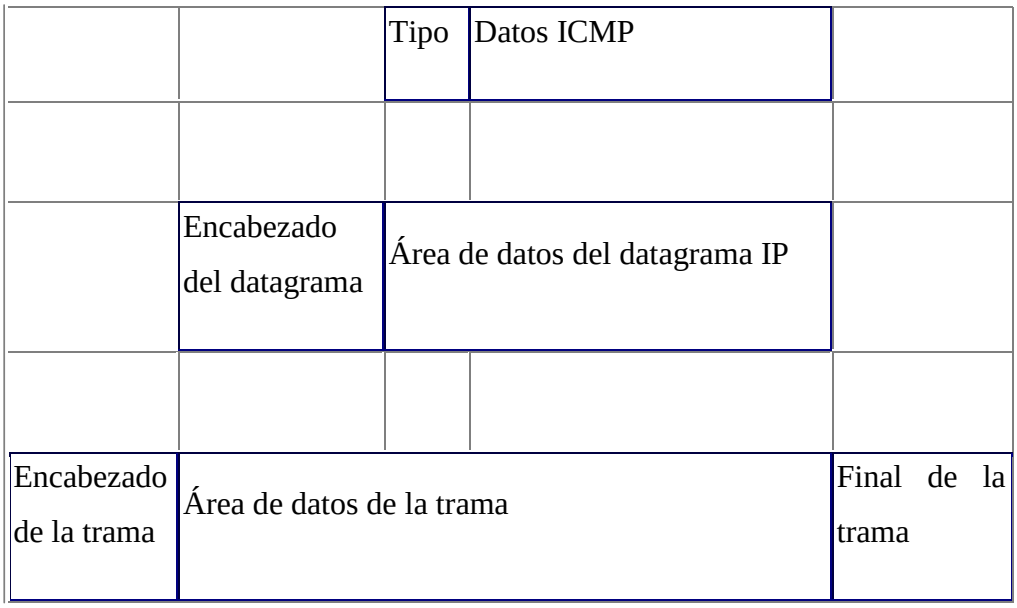


Fig. 1.20 Protocolo ICMP (Protocolo de Mensajes de Control y Error)

Fuente: Kemikal Mayo 2009

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

[60] FMC, 2009.

Los dos protocolos principales de la capa de transporte son UDP y TCP. El primero ofrece una transferencia de mensajes no fiable y no orientada a conexión y el segundo, una transferencia fiable y orientada a conexión. [61]

Protocolo de Transferencia de Archivos (FTP)

Es uno de los protocolos más viejos y populares que se encuentran en el internet hoy en día. Su objetivo es el de transmitir archivos exitosamente entre máquinas en una red sin que el usuario tenga que iniciar una sesión en el host remoto o que requiera tener conocimientos sobre cómo utilizar el sistema remoto. FTP permite a los usuarios acceder a archivos en sistemas remotos usando un conjunto de comandos estándar muy simples.

FTP utiliza una arquitectura cliente/servidor para transferir archivos usando el protocolo de red TCP. Puesto que FTP es un protocolo más antiguo, no utiliza una autenticación de usuarios y contraseña encriptada. Por esta razón, se considera un protocolo inseguro y no se debería utilizar a menos que sea absolutamente necesario. SFTP, del conjunto de herramientas OpenSSH, es un buen sustituto para FTP.

La aplicación FTP tiene dos tipos de ficheros básicos: ASCII y Binarios. Un fichero ASCII o texto estándar es aquel en el que la información que contiene está escrita en caracteres de código ASCII. El binario es cualquier otro tipo de fichero: programas, imágenes, sonidos, etc. Todo esto implica que cuando se realiza una transferencia con FTP debe indicarse el tipo de fichero de que se trata.

Las velocidades de transferencia para FTP dependen de las características de la conexión, como puedan ser los baudios del modem, no es lo mismo utilizar un modem de 2400 baudios que otro a 34600.

Aunque FTP es el protocolo más conocido y utilizado para la transferencia de archivos en Internet, también existen otros protocolos similares como:

[61] Kioskea, 2009.

TFTP (Protocolo Trivial de Transferencia de Archivos)

Este protocolo omite intencionadamente gran parte de las capacidades de FTP y se centra minuciosamente en las operaciones de leer y escribir un archivo, para la ejecución de las cuales utiliza UDP (Protocolo de Datagrama de usuario). A diferencia de FTP no utiliza directorios ni autoriza usuarios. Utiliza un sistema de confirmaciones para asegurar la entrega de datos entre el servidor y el cliente. Es una aplicación muy fácil de implementar y que ocupa muy poco espacio, por lo cual se propuso utilizarlo para transferir bootstrap loaders (programas de arranque).

Protocolo Simple de Transferencia de Archivos (SFTP)

Es un intento por encontrar un punto intermedio entre FTP y TFTP. Soporta el control de acceso, transferencia de archivos, listas de directorios, cambio de directorios, renombramiento y borrado de archivos. Utiliza el protocolo TCP pero con una sola conexión.

FTP emplea dos conexiones TCP para ejecutar las transferencias de archivos, identificando una como conexión de control y otra como conexión de datos. La conexión de control es una configuración cliente/servidor común. El servidor FTP hace una apertura pasiva en el puerto de protocolo 21 y espera las conexiones del cliente. A su vez el cliente contacta al servidor FTP y los programas negocian una conexión TCP, permaneciendo la conexión de control activa durante toda la transacción FTP. FTP crea una conexión de datos independiente para cada transferencia de archivos.

En el núcleo de la operación están los intérpretes de protocolos (PI) y los procesos de transferencia de datos (DTP). Cliente y Servidor tienen cada uno su propio intérprete de protocolos y su propio proceso de transferencia de datos.

Los procesos de transferencia de datos establecen y manejan la conexión de datos. Los intérpretes de protocolo interpretan los comandos FTP y se comunican

a través de la conexión de control, que el PI cliente establece al principio de la sesión.

Manejo de la información.- FTP requiere que los usuarios seleccionen de una gran variedad de opciones para las operaciones de transferencia de archivos. Las opciones de FTP se clasifican en 4 categorías: tipos de archivos, formatos de archivos, estructuras de archivos y modos de transmisión.

Tipos de Archivos: Puede utilizar cuatro tipos de archivos: local, binario, EBCDIC y ASCII.

Formatos de archivo FTP.- Un usuario también debe de especificar un control de formato. FTP define tres tipos de controles de formato: de no impresión, control de formato Telnet y control de carro FORTRAN. Para los archivos de texto, el control predeterminado es el de no impresión.

Modos de Transmisión.- Otra de las características que el usuario debe especificar es el modo de transmisión. FTP define 3 modos de transmisión: de bloque, comprimido y de flujo.

- **De Bloque:** Transfiere un archivo como una serie de bloques, cada uno de los cuales uno o más bytes de encabezado, que especifican el tamaño del bloque enviado, así como los códigos descriptores, que identifican el fin del archivo.
- **Comprimido:** Un algoritmo sencillo de codificación de longitud de ejecución comprime ocurrencias consecutivas del mismo byte, utilizando un símbolo especial seguido por un conteo. Aunque en general la mayoría de los usuarios utilizan algoritmos de compresión, los cuales tienen un mejor funcionamiento.
- **De Flujo:** Se transfiere un archivo como un flujo de bytes de datos. Si el tipo de estructura que se transmite es un registro, FTP utiliza una secuencia especial de caracteres de dos bytes para marcar el fin de un

registro y el fin de un archivo. Mientras que cuando es un archivo, señala su fin al cerrar la conexión de datos TCP.[62]

RIP (Protocolo de Información de Encaminamiento)

Es un protocolo de vector de distancias, es decir que cada router le comunica al resto de los routers la distancia que los separa (la cantidad de saltos que los separa). Por lo tanto, cuando un router recibe uno de estos mensajes incrementa esta distancia en 1, y envía el mensaje a routers directamente accesibles. De esta manera, los routers pueden mantener la ruta óptima de un mensaje, al almacenar la dirección del router siguiente en la tabla de enrutamiento de manera tal que la cantidad de saltos para alcanzar una red se mantenga al mínimo. Sin embargo, este protocolo sólo tiene en cuenta la distancia entre equipos en cuanto a saltos y no considera el estado de la conexión para seleccionar el mejor ancho de banda.

Existen dos versiones de RIP: La versión 1 (RIP-1) es un protocolo ampliamente destacado con sus limitaciones. La versión 2 (RIP-2) es una versión mejorada diseñada para aliviar las limitaciones de RIP hasta que sea altamente compatible con él.

El término se PIR EE.UU. para referirse a la versión 1, mientras que RIP-2 se refiere a la versión 2. Cuando el lector se encuentre el término PIR en la literatura de TCP/IP, debería asumir que se está refiriendo a la versión 1 a menos que explícitamente se diga lo contrario. Esta nomenclatura se usará en esta sección excepto cuando las dos versiones se estén comparando, donde se usará el término RIP-1 para evitar posibles confusiones.

RIP Versión 1

RIP es un protocolo estándar (STD 34). Su estado es electivo. Se describe en el RFC 1058.RIP es una implementación directa del enrutamiento vector-distancia para

[62] Lycos, 2009.

redes locales. La comunicación PIR EE.UU. UDP como protocolo de transporte, con número de puerto 520 como puerto de destino (para una descripción de UDP y puertos). RIP ópera es uno de los dos modos siguientes: activo (normalmente lo usan los routers) y pasivo (normalmente lo usan los hosts).

RIP los mensajes se envían en datagramas UDP y cada uno contiene 25 parejas de números. Se pueden listar entre 1 y 25 rutas en un mensaje PIR. 25 rutas con el mensaje son de 504 bytes (25x20 +4) que es el tamaño máximo del mensaje que puede transmitirse en un datagrama UDP de 512 bytes.

Dirección IP.- Es la dirección IP para esta entrada de enrutamiento: un host o una subred (en cuyo caso el número de host es cero).

Métrica de salto.- Es el número de saltos al destino. El contador de saltos para una interfaz conectada directamente es 1, y cada enrutador intermedio lo incrementa en 1 hasta un máximo de 15, un 16 indica que no existe ruta hacia el destino.

Ambos participantes PIR, activo y pasivo, escuchan todos los mensajes emitidos y actualizan sus tablas de enrutamiento según el algoritmo vector-distancia descrito anteriormente.[63]

RIP-2("Routing Information Protocol" Versión 2)

RIP-2 permiten máscaras de subred de longitud variable (VLSM) en la interconexión. (El estándar RIP-2 permite actualizaciones desencadenadas, a diferencia de RIP-1 La definición del número máximo de rutas paralelas permitidas en la tabla de enrutamiento faculta a RIP para llevar a cabo el equilibrado de carga.

RIP-2 soporta además el multicast con preferencia al broadcastadcast. Esto puede reducir la carga de los host que no están a la escucha de mensajes RIP-2. Esta opción es configurable para cada interfaz para asegurar un uso óptimo de los servicios del RIP-2.

[63] Kioskea, 2009.

1.7.2.1.7 MEDIOS DE TRANSMISIÓN

Dentro de los medios de transmisión, habrá medios guiados y medios no guiados; la diferencia radica que en los medios guiados el canal por el que se transmite las señales son medios físicos, es decir, por medio de un cable; y en los medios no guiados no son medios físicos.[64]

1.7.2.1.7.1 Tipos de Transmisión

Actualmente, la gran mayoría de las redes están conectadas por algún tipo de cableado, que actúa como medio de transmisión por donde pasan las señales entre los equipos, hay disponibles una gran cantidad de tipos de cables para cubrir las necesidades y tamaños de las diferentes redes, desde las más pequeñas a las más grandes. Algunos fabricantes de cables publican unos catálogos con más de 2.000 tipos diferentes que se pueden agrupar en tres grupos principales de las redes:

Medios Guiados:

- Cable coaxial.
- Cable de par trenzado.
- Cable de fibra óptica.[65]

CABLE COAXIAL

Fig. 1.21 Cable Coaxial
Fuente: Tango Delta, 2009.

[64] Wikibooks, 2009.
[65] Lucy, 2009.

El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector.

La construcción del cable coaxial produce una buena combinación y un gran ancho de banda y una excelente inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1km, por ejemplo, es factible obtener velocidades de datos de hasta 10Mbps, y en cables de longitudes menores, es posible obtener velocidades superiores. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de largas distancia del sistema telefónico.[66]

CABLE PAR TRENZADO

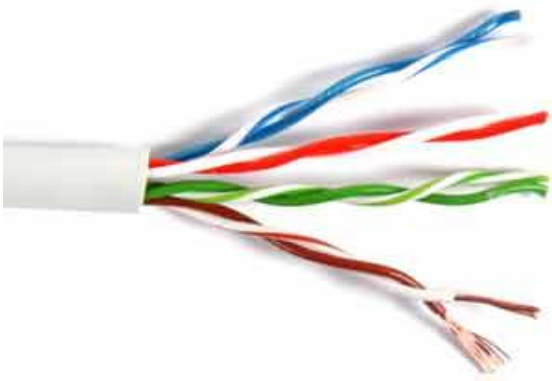


Fig. 1.22 Cable Par Trenzado
Fuente: Carlos Bahoquez, 2009.

El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores más anchos. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías.

[66] Herramienta WEB, 2009.

A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

- Categoría 3, hasta 16 Mbps
- Categoría 4, hasta 20 Mbps
- Categoría 5 y Categoría 5e, hasta 1 Gbps
- Categoría 6, hasta 1 Gbps y más

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (Unshielded Twisted Pair, par trenzado no apantallado)
- STP (Shielded Twisted Pair, par trenzado apantallado)

Los cables UTP son los más utilizados debido a su bajo coste y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un coste elevado y al ser más gruesos son más complicados de instalar.

El cableado que se utiliza es UTP CAT5. El cableado CAT6 es nuevo y difícil encontrarlo en el mercado. Los cables STP se utilizan únicamente para instalaciones puntuales que requieran una calidad de transmisión muy alta.

Cable Par Trenzado Directo

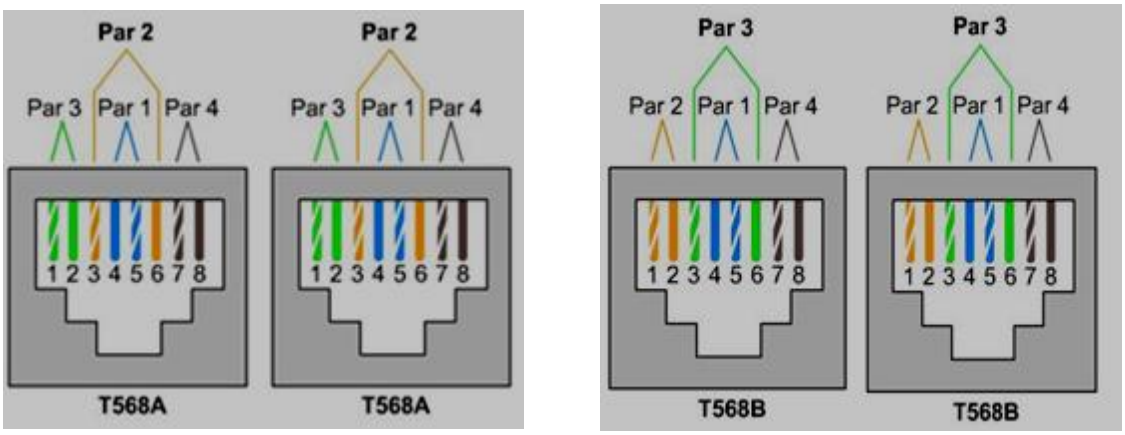


Fig. 1.23 Pares de cables directos

Fuente: David Cotal S., 2009.

Los conectores de cada extremo siguen el mismo estándar. El más común es el T568B con la siguiente combinación de colores: blanco naranja, naranja, blanco verde, azul, blanco azul, verde, blanco marrón y marrón

Estos cables se utilizan para unir: Un computador con hub, una computadora con otra computadora, etc.

Cable Par Trenzado Cruzado

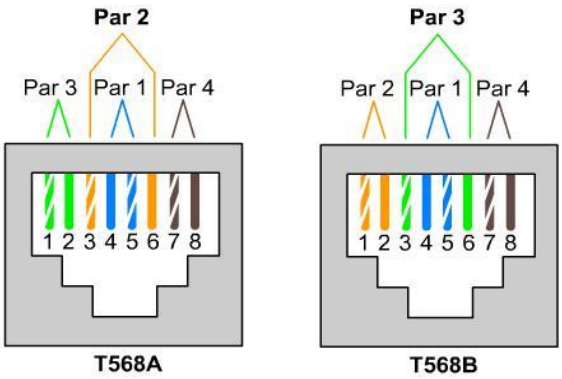


Fig. 1.24 Cable Par Trenzado Cruzado

Fuente: David Cotal S., 2009.

En un extremo del cable se utiliza el estándar anterior y en el otro extremo se utiliza el estándar T568A con la siguiente combinación de colores: blanco verde, verde, blanco naranja, azul, blanco azul, naranja, blanco marrón y marrón

Lo que estamos haciendo es cruzar los pines de transmisión (Tx+ y Tx-) de un extremo con los pines de recepción (Rx+ y Rx-) del otro. Los hilos marcados como N/U no se utilizan.

Estos cables se utilizan para unir:

- 2 computadores sin necesidad de hub (el cable va de una tarjeta de red a la otra).

- 2 hubs (sin utilizar el puerto uplink de ninguno de ellos o utilizando el puerto uplink en ambos).

FIBRA ÓPTICA

Fig. 1.25 Fibra Óptica

Fuente: Lucy Pedro, 2009.

Es una delgada hebra de vidrio o silicio fundido que conduce la luz. Se requieren dos filamentos para una comunicación bi-direccional: TX y RX. El grosor del filamento es comparable al grosor de un cabello humano, es decir, aproximadamente de 0,1mm. En cada filamento de fibra óptica podemos apreciar 3 componentes:

- La fuente de luz: LED o laser.
- El medio transmisor: fibra óptica.
- El detector de luz: fotodiodo.

Un cable de fibra óptica está compuesto por: Núcleo, manto, recubrimiento, tensores y chaqueta.

El cable de fibra óptica, es un medio que se está empezando a utilizar par la interconexión de redes de área local. Aunque es difícil de instalar, de mantener y costoso, se tiene a su utilización por las velocidades que puede alcanzar y la seguridad y fiabilidad de las transmisiones.

La señal que se transmite a través del cable de fibra óptica es luminosa, esta se transmite a través de un cable que está compuesto de fibras de vidrio.

Dentro de la fibra óptica se pueden distinguir las fibras monomodo, en estas el diámetro del núcleo es igual a la longitud de la señal que se transmite, por lo que se consiguen velocidades de transmisión muy altas.

La fibra multimodo, el tamaño del núcleo es mayor, lo que permite que la señal vaya rebotando y se puedan transmitir varios haces a la vez con distinto ángulo de incidencia.

La desventaja que tiene es que al ir rebotando la señal, la velocidad de propagación es menor y la señal se atenúa, otra desventaja es que se puede producir distorsión nodal (rebotes con distintos ángulos de incidencia). La fibra multimodo de índice gradual, consigue que el índice de refracción de la parte interna del cable sea homogéneo con lo que se elimina la distorsión nodal.

Ventajas de la fibra óptica: Puede alcanzar velocidades de transmisión de 1 Gb/seg., tienen gran fiabilidad y seguridad, una gran calidad y resistencia, y como inconvenientes que son muy difíciles de instalar y son muy caras.[67]

MEDIOS NO GUIADOS:

- Radio Enlaces de VHF y UHF
- Ondas de radio.
- Microondas
- Infrarrojos
- Ondas de luz.

Radio Enlaces De VHF Y UHF.- Estas bandas cubren aproximadamente desde 55 a 550 Mhz. Son omnidireccionales, la ionosfera es transparente a ellas. Su alcance máximo es de un centenar de kilómetros, y las velocidades que permite

[67] Lucy, 2009.

del orden de los 9600 bps. Su aplicación suele estar relacionada con los radioaficionados y con equipos de comunicación militares, también la televisión y los aviones.

Ondas de radio.- Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.

Microondas.- Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como satélites. Dada su frecuencia, del orden de 1 a 10 GHz, las microondas son muy direccionales y sólo se pueden emplear en situaciones en que existe una línea visual (punto de vista) que une emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps.

Existen diferentes tipos de enlaces vía radio, y cada uno permite cubrir un rango de distancias a diferentes velocidades de transmisión. No se olvide que en el caso de los enlaces de microondas las distancias, en tierra, de un enlace suelen ser de unos 30 a 50 Km. máximo. Sin embargo, en el caso de la comunicación con un satélite, si bien las distancias pueden ser de hasta 36.000 Km, sólo durante una pequeña parte del recorrido la señal se atenúa por el efecto de la atmósfera y el resto del trayecto es prácticamente en el vacío, que no atenúa la señal. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

Satélite.- Sus ventajas son la libertad geográfica, su alta velocidad, pero sus desventajas son el retardo de las transmisiones debido a tener que viajar grandes distancias. [68]

[68] Wikibooks, 2009.

Infrarrojos.- Son ondas direccionales incapaces de atravesar objetos sólidos (por ejemplo, paredes) que están indicadas para transmisiones de corta distancia.

Ondas cortas.- La OC es una banda de radio, comprendida entre 2 y 15 MHz aproximadamente, (aparece con las siglas SW en los receptores de radio). Poseen un alcance de miles de kilómetros, ya que se reflejan en la ionosfera y además son omnidireccionales, aunque sólo permite reducidas velocidades de transmisión, menores de 1200 bps. Aunque antaño fueron el medio más común, su uso actualmente se encuentra restringido a circunstancias especiales, debido a su limitada capacidad.[69]

Ondas de luz.- Las ondas láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector. En cambio las Microondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. [70]

1.7.2.1.8 EQUIPOS

EQUIPOS ACTIVOS: los equipos electrónicos. Ejemplos: centrales telefónicas, concentradores (hubs), conmutadores (switches), ruteadores (routers), teléfonos, etc.

HUB

Fig. 1.26 HUB

Fuente: Korrerias, 2009.

[69] Galarza, 2007.
[70] Lucy, 2009.

También denominado concentrador. Cuando se transmiten señales eléctricas por un cable, se produce una degeneración proporcional a la longitud del cable, lo que se denomina Atenuación. Un hub es un simple dispositivo que se añade para reforzar la señal del cable y para servir de bus o anillo activo.

Las velocidades de los hubs, van ligadas a las velocidades de la norma Ethernet, es decir, 10, 100 y 1000 Mbps. Es importante tener en cuenta que la velocidad del hub debe ser la misma que posee la tarjeta NIC del computador, a menos que se adquiera los más últimos modelos de hub que aceptan cualquiera de las velocidades de 10 y 100 Mbps, bajo la denominación de autosensing.

Esta característica hace que el puerto del hub o de la NICI se ajuste a la velocidad del otro equipo extremo. Esto se realiza ejecutando un protocolo de pulsos de enlace rápido FLP (Fast Línk Pulses), el cual también define el modo de transmisión half o full duplex.

ROUTER

Fig. 1.27 Router
Fuente: Christian Pérez, 2009

Un router (o enrutador), es un dispositivo de hardware que permite la interconexión de red entre computadores que opera en la capa tres. Un router es un dispositivo que asegura el enrutamiento de paquetes entre redes, o bien determinar la ruta exacta que debería tomar el paquete de datos que intercambiamos.

Por este motivo, los denominados como protocolos de enrutamiento son aquellos que utilizan los routers para comunicarse entre sí, y para permitir el compartimiento de la información, tomando por ende la decisión de cuál es la ruta más adecuada en cada momento para enviar un paquete.[71]

Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.

La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con tablas de enrutamiento actualizadas, que son verdaderos mapas de los itinerarios que pueden seguirse para llegar a la dirección de destino.

Además de su función de enrutar, los routers también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de paquetes de datos, los routers deben fragmentar los paquetes de datos para que puedan viajar libremente.[72]

SWITCH

Fig. 1.28 Switch
Fuente: Nortel Networks, 2009.

O conmutador trabaja en las dos primeras capas del modelo OSI, son dispositivos utilizados para entregar todo el ancho de banda a un segmento de red en una fracción de tiempo. Permite utilizar toda la velocidad inter-red. Un switch en su presentación

[71] TECNOY, 2009.
[72] Kioskea, 2009.

es muy parecido al hub, sólo difiere en su función lógica y en la adición de unos puertos para funciones adicionales. El switch realiza transferencia de tráfico de broadcast y de multicast, pero disminuye el dominio de colisión al mínimo.

Además de los puertos nominales (12 o 24), tienen otros puertos adicionales que sirven para conectar un equipo a una velocidad mayor o para unirlo a otro switch. También se le pueden conectar opcionalmente, módulos para interconexión por fibra óptica.

Los switch manejan las velocidades más estándares de la topología Ethernet, es decir, 10 y 100 Mbps o pueden poseer puertos autosensing. Los puertos adicionales de alta velocidad siempre están por encima de la velocidad de los demás puertos. Por ejemplo, cuando el switch es de 10 Mbps, sus puertos de alta son de 100 Mbps, y cuando son de 100 Mbps los puertos los de alta son de 1000 Mbps. La razón de poseer un puerto a una velocidad mayor es con el fin de proveer un canal que pueda manejar en lo posible todo el troughput que se genera en la comunicación entre dos switch, esto añadido a otra característica muy particular de los switch, el multilink trunking.

Dominio de Colisión. La gran fortaleza del switch que trae como secuencia el manejo de toda la velocidad inter-red entre cada uno de sus puertos, es el manejo del dominio de colisión. A diferencia del concentrador que repite los paquetes a todos los puertos presentando un dominio de colisión muy alto, el switch sólo establece un bus entre el puerto del paquete de origen y el puerto del paquete destino, con esto la colisión depende de la simultaneidad en la transmisión de estos dos puertos y no de los 6, 8, 12, 16, o 24 puertos de los hub.

Multilink trunking. Cuando se poseen puertos de alta velocidad para unir dos switch, es posible mediante esta característica, sumar el ancho de banda disponible por cada puerto con el fin de tener un canal de más alta velocidad. El multilink trunking,

convierte dos enlaces de 100 Mbps entre los switch, en uno único de 200Mbps, con esto se logra mayor acceso entre los dos equipos.[73]

BRIDGES O PUENTE

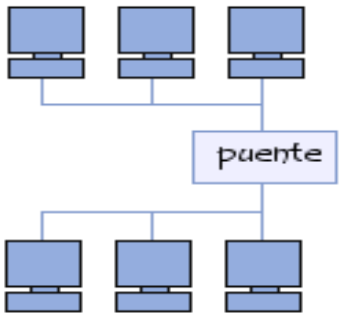


Fig. 1.29 Bridges o Puente

Fuente: Sities Google, 2009

Es un dispositivo de hardware utilizado para conectar dos redes que funcionan con el mismo protocolo. A diferencia de un repetidor, que funciona en el nivel físico, el puente funciona en el nivel lógico (en la capa 2 del modelo OSI). Esto significa que puede filtrar tramas para permitir sólo el paso de aquellas cuyas direcciones de destino se correspondan con un equipo ubicado del otro lado del puente.

El puente, de esta manera, se utiliza para segmentar una red, ya que retiene las tramas destinadas a la red de área local y transmite aquellas destinadas para otras redes. Esto reduce el tráfico (y especialmente las colisiones) en cada una de las redes y aumenta el nivel de privacidad, ya que la información destinada a una red no puede escucharse en el otro extremo.

Sin embargo, el filtrado que lleva a cabo el puente puede provocar una leve demora al ir de una red a otra, razón por la cual los puentes deben ubicarse con buen criterio dentro de una red.

[73] COMPUSOLUSIONES S.A., 2009.

Un puente cuenta con dos conexiones a dos redes distintas. Cuando el puente recibe una trama en una de sus interfaces, analiza la dirección MAC del emisor y del destinatario. Si un puente no reconoce al emisor, almacena su dirección en una tabla para "recordar" en qué lado de la red se encuentra el emisor.

De esta manera, el puente puede averiguar si el emisor y el destinatario se encuentran del mismo lado o en lados opuestos del puente. Si se encuentran en el mismo lado, el puente ignora el mensaje; si se encuentran en lados opuestos, el puente envía la trama a la otra red.

GATEWAY (COMPUERTA O PASARELA)

Fig. 1.30 Gateway (Compuerta o Pasarela)
Fuente: Nortel Networks, 2009.

Una pasarela consiste en una computadora u otro dispositivo que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicaciones, formatos de estructura de datos, lenguajes y/o arquitecturas.

Una pasarela no es como un puente, que simplemente transfiere la información entre dos sistemas sin realizar conversión. Una pasarela modifica el empaquetamiento de la información o su sintaxis para acomodarse al sistema destino. Su trabajo está dirigido al nivel más alto de la referencia OSI, el de aplicación.[74]

REPETIDORES

A medida que las señales eléctricas se transmiten por un cable, tienden a degenerar proporcionalmente a la longitud del cable. Este fenómeno se conoce como

[74] COMPUSOLUCIONES S.A.2009

atenuación. Un repetidor es un dispositivo sencillo que se instala para amplificar las señales del cable, de forma que se pueda extender la longitud de la red.

El repetidor normalmente no modifica la señal, excepto en que la amplifica para poder retransmitirla por el segmento de cable extendido. Algunos repetidores también filtran el ruido. Un repetidor básicamente es un dispositivo "no inteligente" con las siguientes características: Un repetidor regenera las señales de la red para llegar más lejos.

- Se utilizan sobre todo en los sistemas de cableado lineales como Ethernet.
- Los repetidores funcionan sobre el nivel más bajo de la jerarquía de protocolos.
- Se utilizan normalmente dentro de un mismo edificio.
- Los segmentos conectados a un repetidor forman parte de la misma red.
- Los repetidores funcionan normalmente a la misma velocidad de transmisión que las redes que conectan.[75]

Por otra parte, un repetidor puede utilizarse como una interfaz entre dos medios físicos de tipos diferentes, es decir que puede, por ejemplo, conectar un segmento de par trenzado a una línea de fibra óptica.[76]

PUNTO DE ACCESO (ACCESS POINT APs)

Fig. 1.31 Puntos de Acceso (Access Point)

Fuente: Ignacio Pérez, 2007

[75] UTN-FRC. 2009.
[76] Kioskea. 2008.

Los puntos de acceso, también llamados APs o wireless access point son equipos hardware que hace de puente entre la red cableada y la red inalámbrica. Punto de acceso es un dispositivo que podemos añadir a una red existente para dotarla de conectividad inalámbrica. Si ya disponemos de un router, podemos simplemente conectar el punto de acceso a una de sus salidas para así conectar cualquier dispositivo inalámbrico con el resto de la red.

Los puntos de acceso, son generalmente de tamaño pequeño, componiéndose de un adaptador de red, una antena y un transmisor de radio. Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes "ad-hoc" o modo peer-to-peer, las cuales solo utilizan las tarjetas de red para comunicarse. Las redes más usuales son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos wi-fi y una red Ethernet cableada.

También harán la función de escalar a mas usuarios según se necesite y podrá dotar de algunos elementos de seguridad. Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados Wireless Routers los cuales soportan los estándar 802.11a, 802.11b y 802.11g.

Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a él se llama "celda". Usualmente se hace un estudio para que dichas celdas estén lo más cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red.

Si conectamos muchos Access Point juntos, podemos llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad. A nivel casero y como se ha dicho, los puntos

de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable.

Sin embargo debemos ser cautos. Cualquier persona con una tarjeta de red inalámbrica y un portátil puede conectarse a nuestra red Wi-fi y aprovecharse gratuitamente de nuestro ancho de banda. Para evitar esto, el AP puede hacer filtrados por MAC o dirección física no permitiendo la conexión de clientes desconocidos. Muchos de estos dispositivos llevan ya instalado su propio Firewall con el que proteger la red . Para que la integridad de nuestros datos no se vea vulnerada, tenemos la opción de utilizar métodos de encriptación como WEP o la más moderna WPA.[77]

Los puntos de acceso tienen otra importante propiedad, se les puede conectar una antena opcional para aumentar la cobertura inalámbrica que pueden llegar hasta más de 5 km dependiendo del tipo de antena.[78]

EQUIPOS PASIVOS: Elementos no electrónicos de una red. Por ejemplo: cable, conectores, cordones de parcheo, paneles de parcheo, bastidores, etc.

Bastidor (RACK):

Fig. 1.32 Bastidor (Rack)
Fuente: FLYTECH, Octubre 2009

[77] Hewlett Packard, 2009.
[78] 34t, 2009.

Estructura metálica autosoportada, utilizada para montar equipo electrónico y paneles de parcheo. Estructura de soporte de paneles horizontal o vertical abierta afianzada a la pared o el piso. Usualmente de aluminio (o acero) y de 48cms. (19") de ancho por 2.10mts. (7') de alto. Inglés: rack. [79]

HERRAMIENTAS

PIGTAIL (LATIGUILLO)

Es un trozo de cable que lleva en cada uno de sus extremos un conector. Su utilidad es la de unir un dispositivo wireless (punto de acceso, tarjeta PCMCIA, tarjeta pci, etc) a una antena wireless.

Como las pérdidas por atenuación de la señal dentro del cable en la frecuencia de 2.4 GHz son muy altas, se procurará elegir el latiguillo más corto posible y realizado con el cable de mayor calidad que se disponga.

Dependiendo del conector que tenga la antena que vamos a utilizar y del conector que tenga el aparato wireless al que pensemos conectarla tendremos que optar entre los diversos tipos de pigtails. Los Pigtails suelen nombrarse como: "pigtail de equis centímetros de tipo _ conector_ A a tipo z_conector_B"[80]

Fig. 1.33 Pigtail o latiguillo
Fuente: PARAMOWIFIX, 2009

[79] 34TELECOM, 2009.
[80] NUV.2009.

CONECTORES

Conector BNC.- Es el conector utilizado cuando se utiliza cable coaxial. Como ya hemos dicho, la malla de cable coaxial y el hilo central están separados, así que es muy importante que a la hora de grimpar este conector al cable dichos hilos se hallen separados.

Conector RJ-45.- Se utiliza con el cable UTP. Está compuesto de 8 vías con 8 "muelas" que a la hora de grimpar el conector pincharán el cable y harán posible la transmisión de datos.

Por eso será muy importante que todas las muelas queden al ras del conector.

Conector RJ-49.- Igual que el anterior, pero recubierto con una platina metálica para que haga contacto con la que recubre el cable STP.

Conector N-Macho.- Este conector es el más utilizado para realizar conexiones a muchas antenas externas.

Fig. 1.34 Conectores N Macho
Fuente: Seguridades Wireless, 2009

En todos los casos vemos tres partes diferenciadas, el pin interno que sería macho, la carcasa o cuerpo que en este caso también seria macho, y también observamos un cilindro que será usado para crimpar la malla del cable con el chasis del conector.

En el pin interno macho se introducirá el conductor interno de los cables que habitualmente se llama activo, y también su ensamblaje es mediante crimpado.

Cualquier modificación de la instalación para aumentar la cobertura con una antena externa más potente, pasa por usar este conector en uno de los extremos del pigtail.

Conector N-Hembra.- Este conector es el más utilizado por los diferentes fabricantes de antenas comerciales.

Pero hay que distinguir ciertas matizaciones. Es decir existen variantes al mismo.

Entre los conectores N-Hembra podemos encontrarnos tres subclases bastante diferenciadas, todos serán N-Hembra pero mantienen particularidades respecto a su sujeción física.

1. **Conector N-Hembra estándar (sin sujeción física).-** En todos los casos se ve tres partes diferenciadas, el pin interno que sería hembra, la carcasa o cuerpo que en este caso sería también hembra, y también observamos un cilindro que será usado para crimpar la malla del cable con el chasis del conector.

   En el pin interno hembra se introducirá el conductor interno de los cables que habitualmente se llama activo, y también su ensamblaje es mediante crimpado.

Fig. 1.35 Conector N Hembra estándar
Fuente: Seguridades Wireless, 2009

2. Conector N-

Hembra de chasis (sujeción 4 tornillos).- Este conector es el más habitual que nos encontraremos en muchas antenas a partir de cierto nivel de dbi.

También se puede usar para la fabricación de antenas caseras siempre que su salida sea vertical y apoyada en zonas o mejor dicho superficies planas.

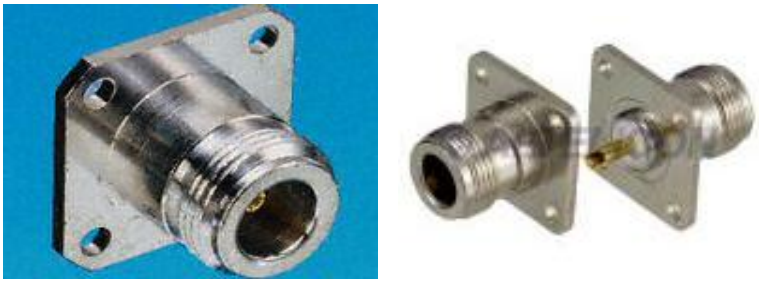


Fig. 1.36 Conector N Hembra de Chasis (sujeción 4 tornillos)

Fuente: Seguridades Wireless, 2009.

Conector N-Hembra de chasis (sujeción solo 1 tuerca).- Este conector sería ideal para usarlo en antenas caseras, ya que incorpora una propia tuerca más arandela para sujeción del mismo, la propia arandela presenta una pestaña (con un pequeño agujero en el lateral) que se puede usar para asegurar la conexión ente la malla del cable wireless y el chasis de la antena, siempre que sea metálico y por lo tanto conductor.

Fig. 1.37 Conector N Hembra de Chasis (sujeción solo 1 tuerca)

Fuente: Seguridades Wireless, 2009

Conector N-Hembra de chasis (sujeción 4 tornillos-montaje araña).- En el conector N-Hembra con tipo de sujeción de cuarto tornillos, la parte trasera seria idéntica a la parte trasera del conector N-Hembra con tipo de sujeción de solo una tuerca + arandela.

Fig. 1.38 Conector N Hembra de Chasis (sujeción 4 tornillos-montaje araña)
Fuente: Seguridades Wireless, 2009

Transceiver ó Tansceptor.- Con estas dos palabras se denomina a un convertidor de medio, o lo que es lo mismo, a un aparato cuya función es la convertir un tipo de cable en otro. Por ejemplo, un TRANSCEIVER de FIBRA ÓPTICA nos convierte la señal de AUI a Fibra óptica.

Cordón de parcheo (patch cable).- Cable de pares torcidos de cobre con conectores machos en ambos extremos, típicamente (RJ-45).

Fig. 1.39 Cordón de parcheo (patch cable)
Fuente: QUEST, 2009

Los cordones de parcheo son utilizados para conectar paneles de equipo pasivo entre sí, paneles de equipo pasivo a equipo activo, salidas de área de trabajo a equipos (típicamente microcomputadoras).

Backbone La parte de la red que conecta la mayoría de los sistemas y redes entre si y maneja la mayoría de los datos.[81]

Dispositivo de testeo.- Son dispositivos que certifican la red es decir que una vez culminado el cableado estos verifican su estado y su funcionamiento.

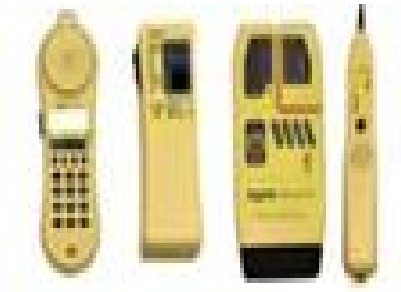


Fig. 1.40 Dispositivo de Testeo
Fuente: Simón Vélez, 2007

Torres y Mástiles

Una torre es una estructura auto-soportada mientras que un mástil es soportado por vientos, riendas o tirantes. Los términos "torres" y "mástil" se utilizan a menudo para el mismo tipo de estructura, lo que por supuesto puede causar confusión.

Tipos de torres

Los tres tipos más comunes de torres que hoy se utilizan en comunicaciones inalámbricas; torres monopolos, auto-soportadas y torres venteadas.

Monopolos

Son postes afilados huecos hechos de acero galvanizado que se construyen de tubos articulados que pueden llegar hasta 60 metros. Debido a su construcción,

[81]PUNTODERED, 2009.

son costosos de fabricar, pero simples de levantar. Se utilizan en ambientes urbanos donde hay espacio limitado disponible para la base de la torre.

La huella máxima de un monopolo de 60m es de unos 2x2 m.

Fig. 1.41 Monopolos

Fuente: Alberto Escudero Pascual, 2007

Torres auto-soportadas

Son caras pero algunas veces son necesarias, particularmente cuando se requiere una gran altura. Pueden ser tan simples como un mástil robusto enterrado en una fundación de concreto.

Una torre auto-soportada (torre libre) se construye sin los tirantes de alambre (vientos).

Las torres auto-soportadas tienen una huella más grande que las monopolos, pero todavía requieren un área mucho más pequeña que las torres venteadas.

Las torres auto-soportadas se pueden construir con tres o cuatro lados. Están formadas por perfiles angulares formando secciones generalmente fabricadas con hierro galvanizado para resistir la corrosión.

Cuanto más ancha es la base de la torre, mayor carga puede tolerar.

Fig. 1.42 Torres Auto-soportadas
Fuente: Alberto Escudero Pascual, 2007

Torres venteadas

A la que se puede trepar es una excelente elección para muchas instalaciones, pero para estructuras muy altas se necesita una torre auto-soportada.

Las torres venteadas son mucho más económicas pero ocupan un área considerable ya que los vientos deben estar anclados a una distancia de la base que es por lo menos la tercera parte la altura.

Estas torres son ideales para cubrir todas las necesidades de comunicaciones, incluyendo Internet inalámbrico, celulares y radiodifusión.

Las torres venteadas se aseguran con tirantes que se anclan en un conjunto de bases de concreto sobre la tierra. Una torre venteada consiste de varios tramos identicos, generalemnte de sección triangular (aproximadamente 3m cada uno) que se apilan uno sobre el otro.

Fig. 1.43 Torres Venteadas

Fuente: Alberto Escudero Pascual, 2007

Espesor de los vientos

Fig. 1.44 Espesor de los vientos

Fuente: Alberto Escudero Pascual, 2007

Los vientos o tirantes se deben elegir de acuerdo a la altura de la torre y a la velocidad esperada del viento en la zona. La parte superior de las colinas, a menudo es el sitio escogido para colocar torres, la velocidad del viento siempre es mayor, sobre todo cuando están desprovistas de árboles.

Tensado de los vientos

Fig. 1.45 Tensado de los vientos
Fuente: Alberto Escudero Pascual, 2007

Es importante que los vientos sean tensados correctamente para que puedan ser efectivos.

Seguridad

Fig. 1.46 Equipo de seguridad
Fuente: Alberto Escudero Pascual, 2007

Cuando se trabaja en alturas utilice siempre arneses de seguridad amarrados a la torre. Cuente siempre con un compañero, y suba sólo cuando haya buena luz. Trabajar en una torre puede llevar más tiempo del que usted piensa y es

extremadamente peligroso trabajar en la oscuridad. Evite trabajar en las torres cuando haya fuertes vientos o tormentas.[82]

Soportes para antenas

A menudo no es necesaria una torre para soportar una antena, sino que es suficiente un tubo sujeto firmemente a alguna estructura. Se emplean tres tipos de instalaciones: montajes para antenas no- penetrantes para el uso en azoteas planas, montaje penetrante y montaje de pared para el uso en las estructuras existentes.

En los techos planos se puede utilizar montajes para la antena que no penetre el piso. Consiste de un trípode colocado en una base de metal o de madera. Luego carga con unos ladrillos, bolsas de arena o cualquier otra cosa pesada. Utilizando este montaje eliminamos la necesidad de perforar el techo, la altura no debe exceder de 3m.

Montaje de pared

Este montaje se pone al lado de un edificio, de una pared o de una chimenea. La estructura debe ser capaz de sostener el peso del mástil, la antena y las fuerzas inducidas por el viento. Este tipo de montaje requiere perforar cuatro agujeros en la estructura. Se puede utilizar tornillos pasantes, cuando tenemos acceso a ambos lados de la estructura.

Cajas herméticas

Fig. 1.47 Cajas Herméticas

Fuente: Alberto Escudero Pascual, 2007

[82] Escudero. 2009.

Las cajas herméticas vienen en muchas variedades. Para crear un contenedor hermético para exteriores se puede usar metal o plástico. El equipo necesita energía para funcionar, y debe ser conectado a una antena y a un cable Ethernet. Cada vez que se perfora un contenedor hermético, se crea un nuevo lugar por el cual puede ingresar el agua. No es imprescindible adquirid una caja profesional para proteger nuestro equipo. Se puede también recitar una caja fabricada para otro propósito, o inclusive fabricar una a bajo costo.

Lo importante es que se protejan bien los agujeros que se practiquen en ella para pasar los cables con este fin se puede utilizar silicón, tanto en la parte interna como en la parte externa del agujero en la caja.

Suministro de energía

La energía DC puede ser provista simplemente haciendo una perforación en la caja y pasando un cable. Si la caja es suficiente grande como una caja eléctrica para exteriores, puede dotarla de un tomacorriente AC, pero los fabricantes están adoptanto una solución muy práctica que elimina la necesidad de una perforación adicional en la caja: Energía a través del cable de Ethernet (PoE).[83]

1.7.2.1.9 ESTÁNDARES DE REDES

Dada la gran variedad de fabricantes y filosofías, para conseguir que el cableado sirva para todas ellas y las que estén por venir, es necesario que exista una normativa en cuanto a lo que va a correr por la red, cómo lo va a hacer y lo que precisa para que esto ocurra. Es vital fijar los parámetros, que deben ser comunes para todos, de tal manera que la forma en la que esté realizada la infraestructura no fije un modo de funcionamiento para cada una de ellas, y además, es preciso que todos los dispositivos (actuales y en desarrollo) se adapten a estas normas.[84]

El comité que se ocupa de los estándares de computadoras a nivel mundial es de la IEEE (Institute of Electrical and Electronics Engineers) una entidad sin fines de lucro, que

[83] Escudero.2009.
[84] Gonzáles, 2009.

reúne a más de 360.000 miembros de 175 países, en su división 802, los cuales se dedican a lo referente de sistema de red entre los que están:

IEEE 802.1: Niveles de aplicación, transporte y red

IEEE 802.2: Subnivel LLC (control de enlaces lógicos) del nivel de enlace[85]

IEEE 802.3 (Ethernet): El comité de la IEEE 802. 3 definió un estándar el cual incluye el formato del paquete de datos para EtherNet, el cableado a usar y el máximo de distancia alcanzable para este tipo de redes. Describe una LAN usando una topología de bus, con un método de acceso al medio llamado CSMA/CD y un cableado coaxial de banda base de 50ohms capaz de manejar datos a una velocidad de 10Mbs.

Ethernet: Es la tecnología de red de área local más extendida en la actualidad. Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX.

Posteriormente en 1.983, fue formalizada por el IEEE como el estándar Ethernet 802.3. La velocidad de transmisión de datos en Ethernet es de 10Mbits/s en las configuraciones habituales pudiendo llegar a ser de 100Mbits/s en las especificaciones Fast Ethernet.

Al principio, sólo se usaba cable coaxial con una topología en BUS, sin embargo esto ha cambiado y ahora se utilizan nuevas tecnologías como el cable de par trenzado y fibra óptica.

La especificación actual se llama IEEE 802.3u. Ethernet/IEEE 802.3, está diseñado de manera que no se puede transmitir más de una información a la vez. El objetivo es que no se pierda ninguna información, y se controla con un sistema conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones), cuyo principio de

[85] García, 2009.

funcionamiento consiste en que una estación, para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza a transmitir.[86]

Se distinguen diferentes variantes de tecnología Ethernet según el tipo y el diámetro de los cables utilizados:

- 10 Base2: el cable que se usa es un cable coaxial delgado RG58, llamado thin Ethernet, banda base y que puede transmitir a 10 Mbps a una distancia de 200 Mts, a esta se le conoce como chip Ethernet.
- 10 Base5: el cable que se usa es un cable coaxial grueso o RG8, llamado thick Ethernet, banda base, que puede transmitir a 10 Mbps a una distancia máxima de 500Mts.
- 10 Base-T: se utilizan dos cables trenzados (la T significa twisted pair) y alcanza una velocidad de 10Mbps.
- 100 Base-FX: permite alcanzar una velocidad de 100 Mbps al usar una fibra óptica multimodo (la F es por Fiber).
- 100 Base-TX: es similar al 10Base-T pero con una velocidad 10 veces mayor (100 Mbps).
- 1000 Base-T: utiliza dos pares de cables trenzados de categoría 5 y permite una velocidad de 1 gigabite por segundo.
- 1000 Base-SX: se basa en fibra óptica multimodo y utiliza una longitud de onda corta (la S es por short) de 850 nanómetros (770 a 860nm).
- 1000 Base-LX: se basa en fibra óptica multimodo y utiliza una longitud de onda larga (la L es por long) de 1350 nanómetros (1270 a 1355nm).[87]

IEEE 802.3af: Energía a través del cable de Ethernet (PoE), define un método para proveer de energia a los dispositivos usando los pares que no se utilizan en un cable Ethernet estándar es decir; para los datos (pares 1-2 y 3-6) y para la energía los no usados (par 4-5 azul/azul-blanco) y (7-8 marrón/marrón-blanco).

[86] IESPANA, 2009.
[87] Kioskea, 2009.

En un cable CAT 5 se pueden suministrar cerca de 13 vatios de forma segura y sin interferir con la transmisión de datos en el mismo cable. [88]

IEEE 802.4 (Token Bus): Hace regencia al método de acceso Token pero para una red con topología en anillo o la conocida como Token bus.

Token bus Sus principales características son:

- Bus de banda ancha.
- Cable coaxial de 75 Ohmios.
- Velocidad de transmisión de 1,5 ó 10Mbps.
- Se trata de una configuración en bus física, pero funcionando como un anillo lógico.
- Todas las estaciones están conectadas a un bus común, sin embargo funcionan como si estuviesen conectadas como un anillo.
- Cada estación conoce la identidad de las estaciones anterior y posterior.

La estación que tiene el testigo, tiene el control sobre el medio y puede transmitir tramas de datos. Cuando la estación ha completado su transmisión, pasa el testigo a la próxima estación del anillo lógico; de esta forma concede a cada estación por turno la posibilidad de transmitir.

El medio se usa alternativamente para fases de transmisión de datos y de paso de testigo. Cada estación puede tener el testigo un tiempo máximo establecido en la red o el tiempo que necesite para efectuar sus transmisiones si es menor.[89]

IEEE 802.5 (Token-Ring): Este estándar define una red con topología de anillo la cual usa token (paquete de datos) para transmitir información a otra. En una estación de trabajo la cual envía un mensaje lo sitúa dentro de un token y lo direcciona específicamente a un destino, la estación destino copia el mensaje y lo envía a un token de regreso a la estación origen la cual borra el mensaje y pasa el token a la siguiente estación.

[88] Escudero, 2009.
[89] Gonzáles, 2009.

IEEE 802.6: Red de área metropolitana (MAN), basada en la topología propuesta por la University of Western Australia, conocida como DQDB (Distribuited Queue Dual Bus) DQDB utiliza un bus dual de fibra óptica como medio de transmisión. Ambos buses son unidireccionales, y en contra-sentido. Con esta tecnología el ancho de banda es distribuido entre los usuarios, de acuerdo a la demanda que existe, en proceso conocido como "inserción de ranuras temporales". Puesto que puede llevar transmisión de datos síncronicos y asíncronicos, soporta aplicaciones de video, voz y datos. IEEE 802.6 con su DQDB, es la alternativa de la IEEE para ISDN[90]

IEEE 802.7: Banda Ancha. Aspectos del nivel físico.

IEEE 802.8 (FDDI): (Fiber Distribuited Data Interfaz) Es un estándar nuevo para redes de área local de alta velocidad. Se trata de un modelo presentado por ANSI y que los organismos internacionales están pensando en normalizar. Sus principales características son:

- Es una red basada en fibra óptica.
- La velocidad de transmisión es de unos 100 Mbps.
- Utiliza una configuración en anillo.
- Puede soportar distancias de hasta 2 Km de fibra óptica entre estaciones, y una circunferencia total de fibra de 200 Km.
- El número máximo de estaciones conectadas es de 500, aunque se pueden conectar dos redes a través de un bridge.
- Habitualmente los enlaces con FDDI se utilizan para unir el concentrador que conecta varias estaciones a un servidor muy potente.
- Utiliza como método de acceso al medio el paso de testigo.

IEEE 802.9: Acceso integrado de voz y datos IVD (Integrated Voice and Data) en la red ISDN o la RDSI (Red Digital de Servicios Integrados, en ingles ISDN) como una evolución de las Redes actuales, que presta conexiones extremo a extremo a nivel

[90] IESPANA, 2009.

digital y capaz de ofertar diferentes servicios. También para ISLAN (Integrated Service LAN) para voz conmutada o en paquetes sobre LAN 802.3.

IEEE 802.10: Seguridad y privacidad en redes locales.

IEEE 802.11: Wireless LAN (Redes Inalámbricas). Método de acceso y nivel físico.

IEEE 802.12: Define el acceso con prioridad por demanda (Demand Priority Access) a una LAN, 100 BaseVG-AnyLAN.

IEEE 802.13: No utilizada.

IEEE 802.14: Define los estándares de módem por cable. [91]

IEEE 802.15: Se enfoca básicamente en el desarrollo de estándares para redes tipo PAN o redes inalámbricas de corta distancia. Al igual que Bluetooth el 802.15 permite que dispositivos inalámbricos portátiles como PCs, PDAs, teléfonos, pagers, entre otros, puedan comunicarse e interoperar uno con el otro.

Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11x, de alguna manera la IEEE definió este estándar para permitir la interoperatibilidad de las redes inalámbricas LAN con las redes tipo PAN. Bluetooth Es la norma que define un Standard global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia.

Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

[91] González, 2009.

IEEE 802.16: Define los estándares sin cable de banda ancha WiMAX es una implementación del estándar que provee conectividad en áreas metropolitanas y velocidades de hasta 75Mb/sec. Los sistemas WiMAX pueden ser utilizados para transmitir señales en distancias tan lejanas como 30 millas. Sin embargo, en promedio un punto de acceso WiMAX cubrirá probablemente entre 3 a 5 millas.

IEEE 802.17: El Grupo de trabajo de Anillos de Paquetes Resilentes del IEEE 802.17 (RPRWG) está abocado a completar la estandarización del Protocolo de acceso de anillos de paquetes resilentes para su utilización en redes de área amplia, local y metropolitana para la transferencia de paquetes de datos a velocidades escalables a gran cantidad de gigabits por segundo. El nuevo estándar utilizará especificaciones existentes de la capa física y, de ser necesario, desarrollará PHY nuevas.

IEEE 802.18: Grupo de Asesoría Técnica sobre Normativas de Radio

IEEE 802.19: Grupo de Asesoría Técnica sobre Coexistencia.

IEEE 802.20: Acceso inalámbrico de Banda ancho móvil, que viene a ser como el 802.16 pero en movimiento.

IEEE 802.21: Interoperabilidad independiente del medio.

IEEE 802.22: Red inalámbrica de área regional.[92]

1.7.2.1.10 ESTÁNDAR EIA / TIA 568

A principios de 1985, las compañías representantes de las industrias de telecomunicaciones y computación se preocupaban por la falta de un estándar para sistemas de cableado de edificio de telecomunicaciones. La Asociación de la industria de Comunicaciones Computacionales (CCIA) solicitó que la Asociación de Industrias

[92] IESPANA, 2009.

Eléctricas (EIA) desarrollara este modelo necesario. En julio de 1991 se publicó la primera versión del estándar como EIA/TIA-568.

Las organizaciones comerciales como la EIA, la IEEE, la BICSI y otras, han desarrollado normas y manuales para estandarizar las telecomunicaciones. La más definida de esas normas es un documento conjunto de la Asociación de la Industria Electrónica y la Asociación de la Industria de las Telecomunicaciones. Después de haber estado en la producción durante seis años y de haber sido aprobado por ANSI en julio de 1991, la "Norma para el cableado de las telecomunicaciones de edificios comerciales EIA/TIA 568" constituye un recurso muy valioso para la industria. Trata sobre la confiabilidad de los equipos, las especificaciones de las pruebas de ejecución de transmisión, las topologías reconocidas y los métodos de instalación y administración.

La norma EIA/TIA 568 define los criterios de desempeño con los cuales se podrían medir con uniformidad todos los accesorios de los fabricantes. Ello obligara a que los fabricantes de accesorios de conexión adopten una posición responsable. No hay tiempo para escuchar una arenga de mercadeo. La industria se va a beneficiar al utilizar criterios objetivos y probados para seleccionar los accesorios de conexión

PROPÓSITO DEL ESTÁNDAR EIA/TIA 568

Los propósitos de este estándar eran principalmente los siguientes:

- Establecer un cableado estándar genérico de telecomunicaciones que respaldará un ambiente multiproveedor.
- Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
- Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableado

La EIA/TIA ha definido el estándar EIA/TIA 568, compuesto de informes técnicos que definen los componentes que hay que utilizar:

- TSB36A: cables con pares trenzados 100W UTP y ftp
- TSB40A: conector RJ45, empalmes por contactos CAD
- TSB 53: cables blindados 150W y conector hermafrodita

Los principales parámetros considerados son: Impedancia, Paradiafonía, Atenuación y ACR (ratio Señal/Ruido). Campo del Estándar EIA/TIA 568-A

El estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina
- Topología y distancias recomendadas
- Parámetros de medios de comunicación que determinan el rendimiento
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años (15 actualmente).

ISO ha desarrollado un cableado estándar sobre una base internacional con el título: Cableado Genérico para Cableado de Establecimientos Comerciales ISO/IEC11801.[93]

1.7.2.1.11 NORMAS ISO

ISO (International Organization for Standarization): Agrupa a 89 países, se trata de una organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia OSI (Open Systems Interconnection) y protocolos estándar para varios niveles del modelo.[94]

ISO/IEC 11801: Especifica sistemas de cableado para telecomunicación de multipropósito cableado estructurado que es utilizable para un amplio rango de aplicaciones (análogas y de telefonía ISDN, varios estándares de comunicación de datos,

[93] W3, 2009.
[94] Galarza, 2007.

construcción de sistemas de control, automatización de fabricación). Cubre tanto cableado de cobre balanceado como cableado de fibra óptica.

El estándar fue diseñado para uso comercial que puede consistir en uno o múltiples edificios en un campus. Fue optimizado para utilizaciones que necesitan hasta 3 km de distancia, hasta 1 km² de espacio de oficinas, con entre 50 y 50.000 personas, pero también puede ser aplicado para instalaciones fuera de este rango.

ISO/IEC 11578:1996 Tecnología de información - Open Systems Interconnection - Remote Procedure Call (RPC)

ISO/IEC 17799 Tecnología de información: Código de la práctica para la gerencia de la seguridad de la información.

ISO/IEC 27001 Tecnología de información - técnicas de la seguridad - sistemas de gerencia de la seguridad de la información – requisitos.[95]

1.7.2.2 REDES INALÁMBRICAS WIRELESS

El desarrollo que ha experimentado Internet actualmente ha creado necesidades de acceso crecientes y cada vez más exigentes por parte de sus usuarios. Tal es así que muchos dependen del acceso para desarrollar parte de su actividad cotidiana, debiendo revisar el correo electrónico permanentemente, recuperar información para completar sus informes, o simplemente buscar un dato o una dirección, por nombrar unos pocos ejemplos. Quienes por su actividad deban desplazarse de un lugar a otro requieren poder acceder a internet en forma simple y desde cualquier ubicación, como los usuarios móviles con sus equipos portátiles en oficinas y bodegas, los que necesitan no solo portabilidad sino movilidad, surgiendo así las redes inalámbricas como una imperiosa necesidad. Para lograr movilidad las computadoras portátiles requieren señales de radio para comunicarse, y así ya no es necesario estar atado a un alambre para conectarse.

[95] WorldLingo Translations LLC, 2009.

La tecnología inalámbrica en la actualidad se ha hecho disponible en muchos lugares públicos como aeropuertos, cafeterías, universidades y otros.

En un principio las redes inalámbricas se desarrollaron en base a radio enlaces, y posteriormente desde el año 1996 aparecieron las primeras redes propietarias portátiles, estando el desarrollo actual normado para que la tecnología pueda ser utilizada independientemente de cuál es el fabricante de los equipos. Las normas han surgido en base a estándares regulados por la IEEE

Habido varios intentos de desarrollo de redes inalámbricas con diferentes tecnologías. Una de ellas es basada en la denominada tecnología infrarrojo, Otra tecnología inalámbrica exitosa es Bluetooth.

Si bien Wi-Fi se creó para acceder a redes LAN en forma inalámbrica, hoy se utiliza mayormente para acceder a Internet. También han surgido los llamados "Hot-Spots" o redes públicas inalámbricas, establecidas en determinados lugares para conectarse a Internet, basadas en Wi-Fi, que corresponde al estándar IEEE 802.11.

Dichos lugares son en general zonas de uso público, en donde es posible acceder a Internet en forma inalámbrica. Hay lugares en que el acceso es compartido gratuitamente, y sólo es necesario acceder a la red inalámbrica para tener acceso a Internet (Free Hot-Spot).

También hay espacios en que se debe cancelar por el acceso. Pero indudablemente una importante aplicación del denominado Wi-Fi es en el hogar, donde puede establecerse fácilmente una red inalámbrica de bajo costo, mediante la cual se puede compartir la impresora o el acceso a Internet desde cualquier ubicación de su casa o departamento y sin tener que romper murallas o desplegar cables. Esta tecnología permite conectarse a una distancia de unos 100 metros o más.

A principios del 2005 se estableció la norma para la denominada WiMax, que está orientada a proveer acceso de banda ancha a nivel metropolitano en forma inalámbrica. La idea es permitir acceso inalámbrico a Internet desde un lugar fijo, compitiendo con

ADSL o cable MODEM. Así, mientras Wi-Fi soporta transmisión en el rango de unos cientos de metros, los sistemas WiMax soportan usuarios en el rango de 30 a 50km.

Ya que todas estas tecnologías están disponibles para el usuario final, debemos advertir que para un mundo convulsionado como el actual, se deben tener precauciones de seguridad para prevenirnos de un uso malintencionado. Al instalar una red inalámbrica, preocúpese de activar las protecciones de acceso que la tecnología le ofrece. [96]

Red inalámbrica: Subred de comunicación con cobertura geográfica limitada, cuyo medio físico de comunicación es el aire. No pretende reemplazar una red cableada, sólo la complementa en situaciones donde es difícil realizar una conexión[97]

Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional.

1.7.2.2.1 ESTÁNDARES WIRELESS

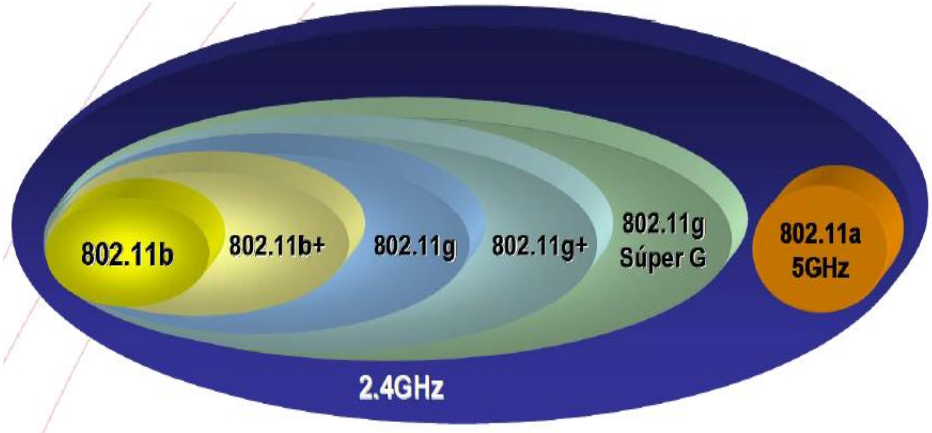


Fig. 1.48 Estándares Wireless

Fuente: Mauro Escalante, 2008

[96] Conozca las redes inalámbricas, 2009.
[97] Lozano, 2009.

IEEE 802.11.- Estándar en operación desde 1999 con producción de equipos poco antes del 2000, este estándar trabaja con Anchos de Banda de 1 a 11Mbps en la banda ISM a 2,4 GHZ.

IEEE 802.11+.- Desarrollo D-Link sobre estándar 802.11b, modulación y como centro de su trabajo el chipset para mejorar el Ancho de Banda, llegando hasta velocidades de 22Mbps.[98]

IEEE 802.11a.- Opera a la frecuencia de 5 GHz, que está menos congestionada que la de 2,4 GHz donde los teléfonos y microondas pueden causar interferencias.

Aunque la velocidad puede llegar hasta 54 Mbps, el alcance es solamente de 75 pies. IEEE 802.11a no es compatible con 802.11b y g ya que opera a diferente frecuencia.

IEEE 802.11a + g.- Linksys también ofrece productos de banda doble, donde los direccionadores y adaptadores son compatibles con ambas frecuencias, 2,4GHz y 5GHz. Ambas bandas de radio trabajan simultáneamente, perturbando su zona inalámbrica y ancho de banda.[99]

IEEE 802.11b.- Es el estándar que se utiliza popularmente para redes inalámbricas de alta velocidad. El estándar está definido por el IEEE (Institute of Electrical and Electronics Engineers) y utiliza una frecuencia de radio 2,4 gigahercios. Hay varias normas que están en uso hoy en día para la comunicación inalámbrica de un computador a otro dispositivo, sin embargo 802.11b es rentable, rápida y fácil de usar.

Esta tecnología normalmente incluye un router inalámbrico que es capaz de enviar señales de radio utilizando 802.11b por el aire a otros equipos o dispositivos electrónicos. Normalmente es un router Wi-fi conectado a un computador o servidor de Internet de banda ancha de conexión. Con el fin de que otros equipos para recoger y enviar señales al router, debe tener una tarjeta Wi-Fi con la capacidad de enviar y recibir señales de 802.11b.

[98] Escalante, 2008.
[99] Neuquén, 2009.

802.11b se ha convertido en un popular estándar inalámbrico Wi-fi por los siguientes atributos:

Velocidad.- 802.11b puede ofrece velocidades de hasta 11 mega bits por segundo, sin embargo esperan una tasa de transferencia típico, cerca de 6,5 mega bits por segundo

Rango.- Esta norma por lo general entrega una señal suficientemente clara para que sea efectiva durante aproximadamente 50 metros (150 pies). Gama puede variar dependiendo de muchas variables, incluyendo, como se estructura en un edificio de apartamentos o edificio de oficinas, tener un router en otro piso de su equipo, que este fuera o en un área abierta y de haber interferencia de otros dispositivos que funcionen cerca de las frecuencias que se utilizado como un horno de microondas o el teléfono inalámbrico.

Claridad de la señal.- Desde 802.11b opera en una frecuencia que es 2,4 -2,5 GHz, la claridad de la señal es buena y porque es más bajo que otras frecuencias, tiene la capacidad para moverse a través de paredes y otros obstáculos, por lo general no se ve afectada.[100]

IEEE 802.11e.- Mejoras en 802.11 para Control de Acceso al Medio (MAC) para mejorar y manejar calidad de servicios, proveer clases de servicios, mejoramientos en la seguridad y los mecanismos de autenticación. Estas mejoras deben proveer la calidad requerida por servicios como telefonía IP y video en demanda.

IEEE 802.11f.- Desarrolla técnicas para un protocolo de Inter-acceso a los puntos (IAPP) para proveer las capacidades necesarias para archivar interoperatibilidad entre puntos de acceso de múltiples vendedores a través de un soporte para un sistema de distribución IEEE P802.11 para link WLAN

IEEE 802.11g.- Es una de las normas utilizadas para las redes inalámbricas de alta velocidad, comúnmente conocido como Wi-fi. Este estándar fue creado por el IEEE (Institute of Electrical and Electronics Engineers), en junio de 2003 y utiliza 2,4 a

[100] TECH-FAQ, 2009.

2,5 gigahercios la frecuencia de radio para enviar y recibir datos de un dispositivo a otro. El estándar 802.11g se está convirtiendo en muy popular durante los últimos años por su velocidad, calidad de transmisión y precio competitivo.

Con el fin de crear una casa o negocio en la red Wi-Fi 802.11g estándar, se necesita un router inalámbrico 802.11g y una tarjeta Wi-Fi compatible con 802.11g. Normalmente es un router Wi-Fi conectado a Internet de banda ancha, ya sea una conexión de un computador o servidor. Con el fin de que cada parte de la red para comunicarse con otro, es necesario que todos ellos tengan una tarjeta Wi-Fi capaz de enviar y recibir señales de 802.11g.

802.11g se ha hecho muy popular como un estándar Wi-Fi en el último par de años debido a 5 grandes atributos. Entre ellas se incluyen la velocidad, alcance, la claridad de la señal, precio y compatibilidad

Velocidad.- La máxima velocidad de 802.11g es de 54 megabits por segundo, sin embargo esperamos que alrededor de 11 megabits por segundo en condiciones normales de un día para otro uso.

Rango.- 802.11g ofrece una gama de cerca de 33 metros o 100 pies aproximadamente. Si bien esta es menor que su primo 802.11b que permite una gama de unos 150 pies, la mayoría de la gente de las redes están bien dentro de los límites de este rango.

Es importante señalar que pueden variar dependiendo de muchos factores, como si una red está instalada en un apartamento, oficina de medio ambiente, si un router está en otro piso de computadores vinculados en la red o si hay interferencia de señales de funcionamiento cerca de 802.11g 's.

Claridad de la señal.- 802.11g opera en la frecuencia 2,4 -2,5 GHz, en su mayor parte, la claridad de la señal es clara y en general, libre de interferencia. Además, esta frecuencia trabaja así penetrar las paredes y otros tipos de obstáculos debido a que opera a bajas frecuencias.

Compatibilidad.- Una gran razón para elegir 802.11g es baja debido a su compatibilidad con 802.11b. La "b" estándar es ampliamente utilizada y "g" puede trabajar de forma integrada con esta norma.[101]

IEEE 802.11g+.- Desarrollo D-Link que permite la mejor utilización de la tecnología proporcionando un Ancho de Banda hasta de 40Mbps.

IEEE 802.11g Súper G.- Desarrollo D-Link que permite una conexión hasta de 108Mbps y con anchos de banda de hasta 60 Mbps (reales), esta tecnología es desarrollada sobre el chipset, también trabaja sobre los 2.4 GHZ

IEEE 802.11h.- Mejoras en 802.11 para control de acceso al medio (MAC) estándar y 802.11A con alta velocidad en la capa física en la banda de los 5 GHZ.

El objetivo es crear un IEEE 802.11ah, productos compatibles con las regulaciones europeas.

IEEE 802.11i.- Mejoras en 802.11 para control de acceso al medio mejorando en si los mecanismos de autenticación y encriptación de datos (seguridad) WEP.[102]

WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key.

IEEE 802.11j.- Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

IEEE 802.11m.- Estándar propuesto para el mantenimiento de las redes inalámbricas.

IEEE 802.11n.- La próxima generación de redes inalámbricas (Wi-Fi) de alta velocidad, capaz de ofrecer el alcance y la capacidad para la mayoría de las aplicaciones actuales hambrientas de ancho de banda, como reproducción de vídeos de alta definición, voz y música.

[101] TECH-FAQ, 2009.
[102] Escalante, 2008.

Actualmente aprobada para el estatus preliminar 1.0 por el comité de tareas grupo-N del IEEE (Instituto de Ingenieros Electrónicos y Eléctricos).

La tecnología n está basada en la tecnología MIMO (múltiples entradas, múltiples salidas), que a su vez usan múltiples señales de radio para transmitir y recibir simultáneamente por varios canales a fin de maximizar el rendimiento de la red inalámbrica.

Aunque MIMO en sí no es un estándar, es la tecnología subyacente que está detrás del aumento de rendimiento en 802.11n.

Estas múltiples señales de radio transmiten múltiples flujos de datos llamados "corrientes espaciales". Cuanto mayor sea el número de corrientes espaciales, mayor será el rendimiento.

Numerosas corrientes de contenido pueden moverse por el mismo canal al mismo tiempo, multiplicando la capacidad de cada canal. La tecnología 802.11n puede duplicar la capacidad usando opcionalmente dos canales de 20MHz.

Con la tecnología de "antena inteligente", se combinan señales intensas, débiles y reflejadas en una transferencia de datos para conseguir el máximo alcance, eliminando casi por completo los puntos muertos en toda su casa u oficina. Este estándar operaría en la banda de 2,4GHz a una velocidad de 108Mbps. [103]

1.7.2.2.2 Wireless LAN (Red de área local inalámbrica)

Características más importantes

- Velocidades, desde 11Mbps hasta 54Mbps (según estándar)
- Red sin cable
- Mismo tipo de aplicaciones y
- Mismo tipo de uso que red cableada

[103] Neuquén, 2009.

Una red de área local o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio e infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, etc).

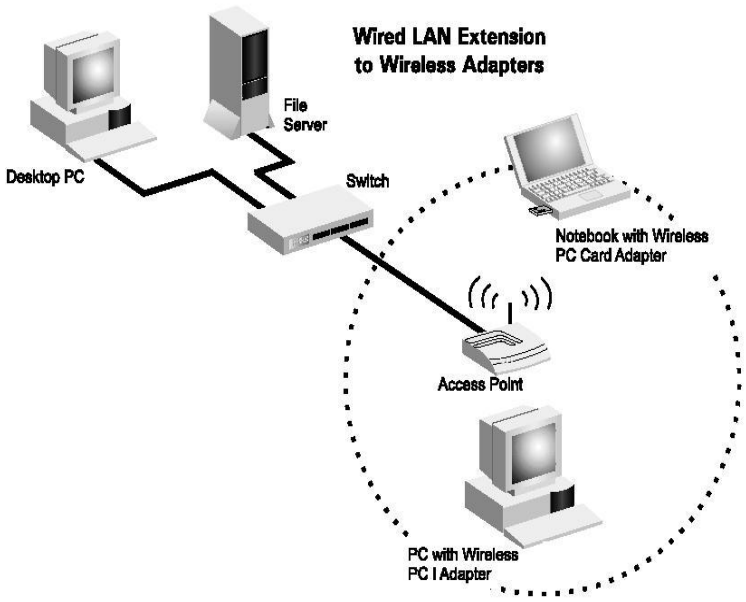


Fig. 1.49 Wireless LAN (Red de Área Local Inalámbrica)
Fuente: Ignacio Pérez, 2007

Las redes locales inalámbricas más que una sustitución de las LANs convencionales son una extensión de las mismas, ya que permite el intercambio de información entre los distintos medios en una forma transparente al usuario.[104]

En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas.

Enlazando los diferentes equipos o terminales móviles asociados a la red. [105]

[104] Escalante, 2008
[105] Hacker Friendly LLC, 2008.

1.7.2.2.3 Dispositivos WLAN

Actualmente se dispone de multitud de dispositivos para conseguir un acceso a una red Wireless, dependiendo del dispositivo desde el que se realice la conexión. Un equipo conectado a una red se denomina host.

a) **Acceso desde un computador portátil o Tablet PC.-** Si el portátil no está equipado con procesadores en los que ya está integrado el adaptador wireless, disponen de ranuras PCMCIA donde conectar las tarjetas. Hay PCMCIA con conector para poder añadir una antena exterior de mayor ganancia.

Fig. 1.50 Tarjeta PCMCIA
Fuente: Ignacio Pérez, 2007

b) **Acceso desde un computador de escritorio.-** En este caso disponemos de varias soluciones dependiendo de nuestras necesidades. Existen tarjetas PCI para pinchar en el interior del equipo, las cuales pueden disponer de una pequeña antena exterior.

Fig. 1.51 Tarjeta PCI para computador de escritorio
Fuente: Ignacio Pérez, 2007

O bien tarjetas PCI puente donde se puede insertar la tarjeta PCMCIA Wireless que se utiliza en los portátiles, de esta manera una misma tarjeta PCMCIA puede tener dos usos.

Fig. 1.52 Tarjeta PCI puente
Fuente: Ignacio Pérez, 2007

Si no desea abrir el computador para pinchar la tarjeta, se puede utilizar adaptadores Wireless USB. Estos tienen la ventaja de poder mover el adaptador para conseguir una mejor señal, ya que se puede utilizar un cable USB más largo.

Fig. 1.53 Adaptador Wireless USB
Fuente: Ignacio Pérez, 2007

La última novedad en cuanto a dispositivos Wireless son los Stick de memoria USB que a su vez son adaptadores Wireless.[106]

Fig. 1.54 Stick de memoria USB
Fuente: Creación Propia

1.7.2.2.4 TOPOLOGÍA INALÁMBRICA

El grado de complejidad de una red de área local inalámbrica es variable dependiendo de las necesidades y características de los equipos que estamos usando o a los cuales accedamos, existen 2 formas básicas de configuración:

- Ad-hoc o peer to peer[107]
- Puntos de acceso o infraestructura

Topología Ad-hoc o PEER TO PEER

Es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

[106] Pérez, 2007.
[107] Escalante, 2008.

En la topología ad hoc los equipos cliente inalámbrico se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

Fig. 1.55 Topología Ad-hoc o Peer to Peer

Fuente: Ignacio Pérez, 2007

Topología Punto de Acceso o Infraestructura

Estas configuraciones utilizan el concepto de celda. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que las redes inalámbricas esta celda suele tener un tamaño reducido.

Fig. 1.56 Topología Punto de Acceso

Fuente: Jaime Llorent Mauri, 2009

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados Puntos de acceso, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los Puntos de acceso son colocados normalmente en alto, pero solo es necesario que estén situados para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros.

La técnica de Punto de acceso es capaz de dotar a una red inalámbrica de muchas posibilidades, además del evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como roaming, es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas.

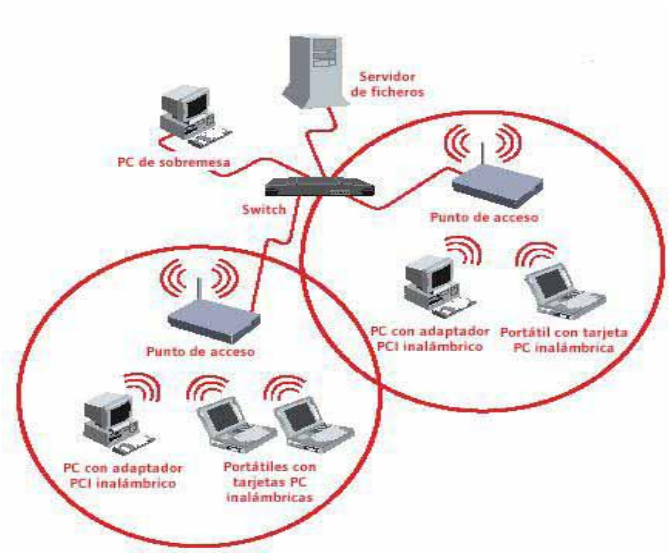


Fig. 1.57 Roaming

Fuente: Ignacio Pérez, 2007

Otras Configuraciones: Interconexión de Redes.- Las posibilidades de las redes inalámbricas pueden verse ampliadas gracias a la interconexión con otras redes, sobre todo con redes no inalámbricas. De esta forma los recursos disponibles en ambas redes se amplían.

Mediante el uso de antenas (direccionales u omnidireccionales) es posible conectar dos redes separadas por varios cientos de metros, como por ejemplo dos redes locales situadas en dos edificios distintos.

De esta forma, una LAN no inalámbrica se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serian más costosas, o simplemente imposibles

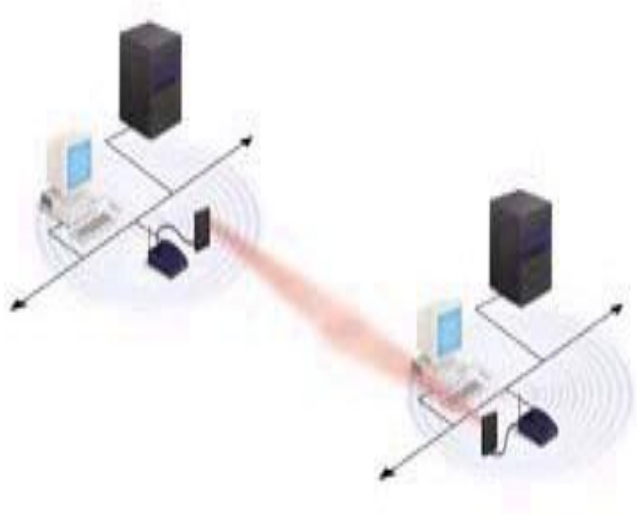


Fig. 1.58 Interconexión de redes.
Fuente: Jaime Llorent Mauri, 2009

Topología: WDS (Wireless Distribution System)

Cuando se diseñó el estándar 802.11 se pensó en dos tipos básicos de servicios:

BSS (Basic Service Set).- En este caso sólo hay un punto de acceso y una red inalámbrica definida por las estaciones conectadas a ese único AP.

ESS (Extended Service Set): en éste caso hay varios APs e interesa que las estaciones conectadas a cualquiera de ellos puedan interconectarse de forma transparente.

El sistema que permite dicha interconexión es el DS (Distribution System).

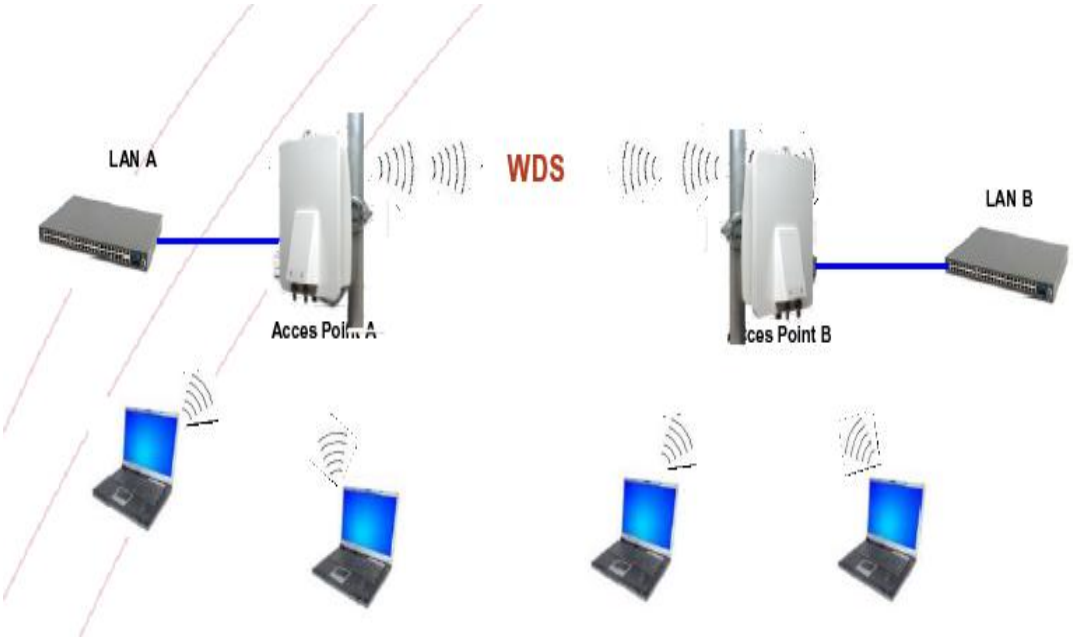


Fig. 1.59 Topología WDS (Wireless Distribution System)

Fuente: Mauro Escalante, 2008

Campos adicionales en el paquete WDS

Las conexiones wireless entre dos estaciones se realizan siempre enviando la dirección MAC de la tarjeta wireless del origen y del destino. La dirección MAC del destino sirve para que la tarjeta del receptor reciba y procese el paquete localmente.

Es decir, estos tipos de paquetes estándares sólo permiten la conexión entre un par de computadores, normalmente un AP y una estación registrada.

En el caso que se quieran interconectara Nivel 2 un par de redes LAN, estos datos no bastan. Suponga el siguiente caso, donde un computador A envía un paquete de datos a otro computador B en otra LAN distinta, interconectada por un enlace inalámbrico.[108]

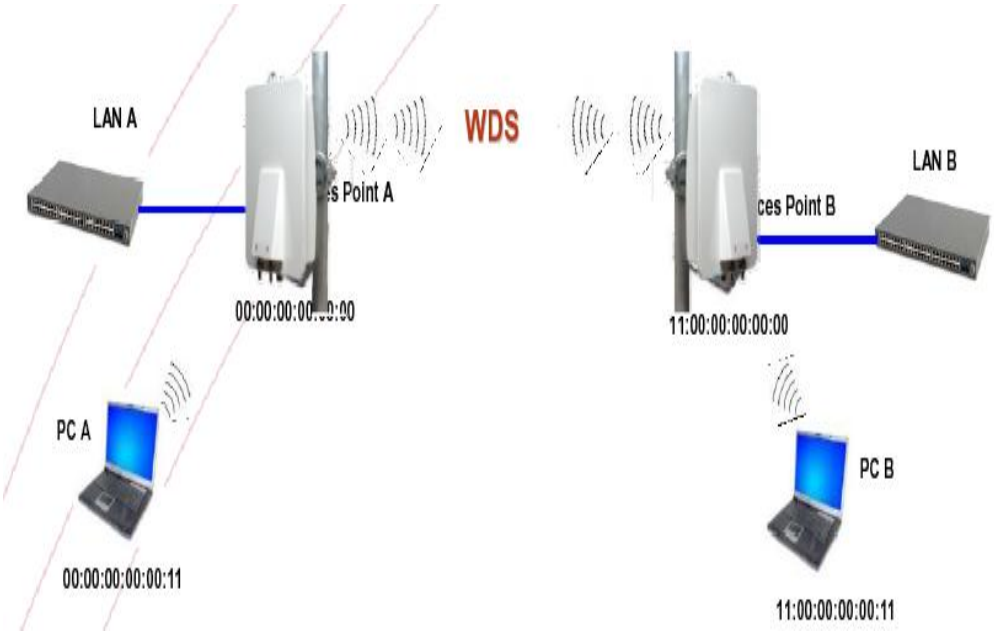


Fig. 1.60 Campos adicionales en el paquete WDS

Fuente: Mauro Escalante, 2008

1.7.2.2.5 WI-FI (Wireless Fidelity)

ORIGEN.- Según Phil Belanger (miembro fundador de la Wi-Fi Alliance que presidió la elección del nombre "Wi-Fi"). Wi-Fi no es abreviatura de nada. No es un acrónimo. No hay significado.

Fig. 1.61 WI-FI

Fuente: Serrano, 2009.

[108] Escalante, 2008.

Wi-Fi y el logotipo a lo ying-yang fueron inventados por Interbrand. (Los miembros fundadores de la Wireless Ethernet Compatibility Alliance, ahora conocida como Wi-Fi Alliance) contrataron a Interbrand para que proporcione un nombre y logotipo que pudiésemos utilizar en nuestra marca de intercompatibilidad y para el marketing. Necesitábamos algo más pegadizo que "IEEE 802.11b Secuencia Directa". Interbrand inventó los nombres "Prozac", "Compaq", "oneworld", "Imation" y muchos otros nombres que son comunes. Incluso crearon el nombre de compañía "Vivato".

La única razón por la que se escucha algo sobre "Wireless Fidelity" es porque algunos de mis colegas tenían miedo. No entendían de marcas o marketing. No podían imaginar el uso del nombre "Wi-Fi" sin tener asociado algún tipo de explicación literal. Así que llegamos a un acuerdo para incluir la frase "The Standard for Wireless Fidelity" (NdT: algo así como el estándar para la fidelidad inalámbrica) al nombre.

Esto fue un error y sólo sirvió para confundir a la gente y diluir la marca. Más o menos durante el primer año (circa 2000) esto aparecería en todas nuestras comunicaciones. Aún tengo un sombrero y un par de polos de golf con la frase. Después, conforme Wi-Fi se iba convirtiendo en un éxito y se tuvo a gente de marketing y negocios de compañías más grandes en la junta, la alianza se deshizo de la frase.

La frase se inventó tras el nombre. Wi-Fi fue de una lista de diez nombres que propuso Interbrand. La frase fue inventada por los primeros seis miembros de la junta y además no significa nada. Si se analiza la frase, se cae por su propio peso: ¿estándar? La Alianza Wi-Fi siempre ha sido muy escrupulosa en permanecer al margen de inventar estándares: el estándar de interés es IEEE 802.11.

La alianza se centra en la interoperabilidad y certificación. No inventa estándares, no compite con IEEE. Se complementan. Así que Wi-Fi no puede ser jamás un estándar. Y ¿fidelidad inalámbrica? ¿Eso qué significa? Nada. Fue un torpe intento de obtener dos palabras que encajasen con Wi y Fi. Sólo eso. [109]

[109] Serrano, 2009.

WIRELESS FIDELITY (Wi-Fi)

Literalmente significa Fidelidad inalámbrica. Es un conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos. Si bien fue creado para acceder a redes locales inalámbricas, hoy es muy frecuente que sea utilizado para establecer conexiones a Internet.

Wi-Fi es una marca de la compañía Wi-Fi Alliance que está a cargo de certificar que los equipos cumplan con la normativa vigente (que en el caso de esta tecnología es la IEEE 802.11).

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

Al año siguiente de su creación la WECA certificó que todos los aparatos que tengan el sello Wi-Fi serán compatibles entre sí ya que están de acuerdo con los criterios estipulados en el protocolo que establece la norma IEEE 802.11.

En concreto, esta tecnología permite a los usuarios establecer conexiones a Internet sin ningún tipo de cables y puede encontrarse en cualquier lugar que se haya establecido un "punto caliente" o hotspot Wi-Fi.

Actualmente existen tres tipos de conexiones y hay una cuarta en estudio

- El primero es el estándar IEEE 802.11b que opera en la banda de 2,4 GHz a una velocidad de hasta 11Mbps.
- El segundo es el IEEE 802.11g que también opera en la banda de 2,4 GHz, pero a una velocidad mayor, alcanzando hasta los 54Mbps.
- El tercero, que está en uso es el estándar IEEE 802.11a que se le conoce como Wi-Fi 5, ya que opera en la banda de 5 GHz, a una velocidad de 54Mbps. Una de

las principales ventajas de esta conexión es que cuenta con menos interferencias que los que operan en las bandas de 2,4 GHz ya que no comparte la banda de operaciones con otras tecnologías como los Bluetooth.

- El cuarto, y que aún se encuentra en estudio, es el IEEE 802.11n que operaría en la banda de 2,4 GHz a una velocidad de 108Mbps.

Para contar con este tipo de tecnología es necesario disponer de un punto de acceso que se conecte al módem y un dispositivo Wi-Fi conectado al equipo. Aunque el sistema de conexión es bastante sencillo, trae aparejado riesgos ya que no es difícil interceptar la información que circula por medio del aire. Para evitar este problema se recomienda la encriptación de la información.

Actualmente, en muchas ciudades se han instalados nodos Wi-Fi que permiten la conexión a los usuarios. Cada vez es más común ver personas que pueden conectarse a internet desde cafés, estaciones de metro y bibliotecas, entre muchos otros lugares.[110]

1.7.2.2.6 SEGURIDAD EN REDES INALÁMBRICAS

Son muchos los motivos para preocuparse por la seguridad de una red inalámbrica. Por ejemplo, queremos evitar compartir nuestro ancho de banda públicamente. A nadie con algo de experiencia se le escapa que las redes inalámbricas utilizan un medio inseguro para sus comunicaciones y esto tiene sus repercusiones en la seguridad. Tendrá situaciones en las que precisamente quiera compartir públicamente el acceso a través de la red inalámbrica, pero también podrá configurar una red inalámbrica para limitar el acceso en función de unas credenciales.

También tenemos que tener en cuenta que las tramas circulan de forma pública y en consecuencia cualquiera que estuviera en el espacio cubierto por la red, y con unos medios simples, podría capturar las tramas y ver el tráfico de la red.

Para resolver los problemas de seguridad que presenta una red inalámbrica se tendrá que poner, por un lado, garantizar el acceso mediante algún tipo de credencial a la red y por

[110] MIS RESPUESTAS, 2009.

otro garantizar la privacidad de las comunicaciones aunque se hagan a través de un medio inseguro.

Una empresa no debería utilizar redes inalámbricas para sus comunicaciones si tiene información valiosa en su red que desea mantener segura y no ha tomado las medidas de protección adecuadas. Cuando utiliza una página web para enviar un número de tarjeta de crédito deberemos, hacerlo siempre utilizando una web segura porque eso garantiza que se transmite cifrada.

Pues en una red inalámbrica tendría que hacerse de una forma parecida para toda la información que circula, para que proporcione al menos la misma seguridad que un cable. Pensemos que en una red inalámbrica abierta se podría llegar a acceder a los recursos de red compartidos.

1.7.2.2.6.1. WEP

WEP (Wired Equivalent Privacy), que viene a significar Privacidad Equivalente a Cable, es un sistema que forma parte del estándar 802.11 desde sus orígenes. Es el sistema más simple de cifrado y lo admiten, creo, la totalidad de los adaptadores inalámbricos. El cifrado WEP se realiza en la capa MAC del adaptador de red inalámbrico o en el punto de acceso, utilizando claves compartidas de 64 o 128 bits.

Cada clave consta de dos partes, una de las cuales la tiene que configurar el usuario/administrador en cada uno de los adaptadores o puntos de acceso de la red. La otra parte se genera automáticamente y se denomina vector de inicialización (IV). El objetivo del vector de inicialización es obtener claves distintas para cada trama. Ahora vamos a ver una descripción del funcionamiento del cifrado WEP.

Cuando tenemos activo el cifrado WEP en cualquier dispositivo inalámbrico, bien sea una adaptador de red o un punto de acceso, estamos forzando que el emisor cifre los datos y el CRC de la trama 802.11. El receptor recoge y la descifra. Para no incurrir en errores de concepto, esto es sólo aplicable a comunicaciones estaciones 802.11, cuando el punto de acceso recoge una trama y la envía a través del cable, la envía sin cifrar.

El cifrado se lleva a cabo partiendo de la clave compartida entre dispositivos que, como indicamos con anterioridad, previamente se tiene que configurar en cada una de las estaciones. En realidad un sistema WEP almacena cuatro contraseñas y mediante un índice indicamos cuál de ellas vamos a utilizar en las comunicaciones.

El proceso de cifrado WEP agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con un la clave compartida para generar la llave de cifrado. Observe como al configurar WEP se tiene que introducir un valor de 40 bits (cinco dígitos hexadecimales), que junto con los 24 bits del IV obtenemos la clave de 64 bits. El vector de inicialización podría cambiar en cada trama trasmitida.

WEP usa la llave de cifrado para generar la salida de datos que serán, los datos cifrados más 32 bits para la comprobación de la integridad, denominada ICV (integrity check value). El valor ICV se utiliza en la estación receptora donde se recalcula y se compara con el del emisor para comprobar si ha habido alguna modificación y tomar una decisión, que puede ser rechazar el paquete.

Para cifrar los datos WEP utiliza el algoritmo RC4, que básicamente consiste en generar un flujo de bits a partir de la clave generada, que utiliza como semilla, y realizar una operación XOR entre este flujo de bits y los datos que tiene que cifrar. El valor IV garantiza que el flujo de bits no sea siempre el mismo. WEP incluye el IV en la parte no cifrada de la trama, lo que aumenta la inseguridad. La estación receptora utiliza este IV con la clave compartida para descifrar la parte cifrada de la trama.

Lo más habitual es utilizar IV diferentes para transmitir cada trama aunque esto no es un requisito de 801.11. El cambio del valor IV mejora la seguridad del cifrado WEP dificultando que se pueda averiguar la contraseña capturando tramas, aunque a pesar de todo sigue siendo inseguro.

Debilidades de WEP

Las debilidades de WEP se basan en que, por un lado, las claves permanecen estáticas y por otro lado los 24 bits de IV son insuficientes y se transmiten sin cifrar. Aunque el

algoritmo RC4 no esté considerado de los más seguros, en este caso la debilidad de WEP no es culpa de RC4, sino de su propio diseño.

Si tenemos un vector de inicialización de 24 bits tendremos 2^24 posibles IV distintos y no es difícil encontrar distintos paquetes generados con el mismo IV. Si la red tiene bastante tráfico estas repeticiones se dan con cierta frecuencia. Un atacante puede recopilar suficientes paquetes similares cifrados con el mismo IV y utilizarlos para determinar el valor del flujo de bits y de la clave compartida. El valor del IV se transmite sin cifrar por lo que es público.

Esto puede parecer muy complicado, pero hay programas que lo hacen automáticamente y en horas o días averiguan la contraseña compartida. No olvidemos que aunque la red tenga poco tráfico el atacante puede generarlo mediante ciertas aplicaciones.

Una vez que alguien ha conseguido descifrar la contraseña WEP tiene el mismo acceso a la red que si pudiera conectarse a ella mediante cable. Si la red está configurada con un servidor DHCP, entonces el acceso es inmediato, y si no tenemos servidor DHCP pues al atacante le puede llevar cinco minutos más.

Vista la debilidad real de WEP lo ideal es que se utilizaran claves WEP dinámicas, que cambiaran cada cierto tiempo lo que haría materialmente imposible utilizar este sistema para asaltar una red inalámbrica, pero 802.11 no establece ningún mecanismo que admita el intercambio de claves entre estaciones.

En una red puede ser tedioso, simplemente inviable, ir estación por estación cambiando la contraseña y en consecuencia es habitual que no se modifiquen, lo que facilita su descifrado.

Algunos adaptadores sólo admiten cifrado WEP por lo que a pesar de su inseguridad puede ser mejor que nada. Al menos evitaremos conexiones en abierto incluso evitaremos conexiones y desconexiones a la red si hay varias redes inalámbricas disponibles. [111]

[111] Fábrega, 2009.

1.7.2.2.6.2. WPA

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente maduro y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto.

El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

EAP, definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).

TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.

MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC. Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de

una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

1.7.2.2.6.3. WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2. Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2

incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).[112]

1.7.2.2.6.4. El filtrado de direcciones MAC

Cada tarjeta de red posee una dirección MAC única, para conocerla (bajo Windows): Menú Inicio > Ejecutar > escribir cmd luego en el prompt escribir ipconfig /all. El router Wi-Fi por lo general permite crear una lista de direcciones MAC de las tarjetas de red que están autorizadas a conectarse a nuestra red. Es un filtro eficaz pero que también puede ser vulnerado pero con mayor dificultad.

Es importante entender que cada uno de estos puntos puede ser vulnerado. En realidad, es la combinación de todos estos puntos que va a hacer de tu red una red más segura. No debemos basar la seguridad de nuestra red en uno solo de estos elementos. Lo mínimo que se recomienda es la WEP y un filtrado de direcciones MAC.[113]

1.7.2.2.7 WIMAX (Interoperabilidad Mundial Para Acceso Por Microondas)

Fig. 1.62 WIMAX

Fuente: Almalasi, marzo 2009

WiMAX está pensado principalmente como tecnología de "última milla" y se puede usar para enlaces de acceso, MAN o incluso WAN. Destaca WiMAX por su capacidad como tecnología portadora, sobre la que se puede transportar IP, TDM, T1/E1, ATM, Frame

[112] Barajas, 2009.
[113] Vialfa, 2008.

Relay y voz, lo que la hace perfectamente adecuada para entornos de grandes redes corporativas de voz y datos así como para operadores de telecomunicaciones.[114]

WiMAX permite la recepción de datos mediante microondas y la retransmisión mediante ondas de radio. Esto facilita el acceso no solo en zonas de población, sino también en zonas aisladas.

El estándar utilizado es el 802.16, con sus respectivas variantes. Este estándar está regulado por el WiMAX Forum, asociación sin ánimo de lucro, encargada del desarrollo y control de la compatibilidad e interoperatibilidad de los diferentes elementos que intervienen es esta tecnología (antenas, routers, receptores).

Hasta el momento, las variantes de este estándar son las siguientes:

802.16 (2002).- Utiliza espectro licenciado en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbps en distancias de 3.22 a 8.05kilómetros. Soporta calidad de servicio (QoS).

802.16a (2003).- Ampliación del estándar 802.16 a bandas de 2 a 11 GHz, con sistemas NLOS y LOS, y protocolo PTP y PTMP.

802.16b (2003).- Delimita redes de área metropolitana inalámbricas en bandas de frecuencia desde 10 a 60GHz.

802.16c (2003).- Ampliación del estándar 802.16 para definir las características y especificaciones en la banda de 10-66GHz.

802.16d (junio de 2004).- Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16 - 2004 últimas versiones.

802.16e (diciembre de 2005).- Extensión del 802.16 que incluye la conexión de banda ancha nómada para elementos portables (computadores portátiles, PDA, móviles...).

[114] WIMAXTECH, 2009

En la actualidad están vigentes la 802.16d, perteneciente a las conexiones WiMAX fijas y la 802.16e, que regula las conexiones WiMAX móviles.

Características principales de WiMAX:

Las características principales de las redes WiMAX son:

- Capa MAC con soporte de múltiples especificaciones físicas (PHY).
- Distancias de hasta 50kilómetros (teórica).
- Velocidades de hasta 70Mbps.
- Facilidades para añadir más canales.
- Anchos de banda configurables y no cerrados.
- Soporte nativo para calidad de servicio (QoS).

El soporte nativo para QoS consiste en una reserva (cuando se necesita) de ancho de banda para una aplicación determinada, y es imprescindible para VoIP o ciertas aplicaciones multimedia.

En la práctica, actualmente las redes WiMAX se dividen en dos:

WiMAX fija.- Bajo el protocolo 802.16d, que funciona mediante antenas fijas (similares a las de TV).

WiMAX móvil.- Bajo el protocolo 802.16e, que trabaja en la banda de 2 - 3 GHz, con una velocidad máxima de 30 Mbps y un rango de hasta 3.5Km.

Las redes WiMAX son redes que trabajan bajo la tecnología NLOS (es decir, que no necesitan tener una línea de visibilidad entre las antenas), pero en la práctica este sistema solo permite atravesar pequeños obstáculos (una casa pequeña, árboles, pequeños muros), pero no puede atravesar obstáculos mayores, como un edificio o una montaña. Además, cuando no hay una línea de visión directa (LOS) entre ambos, tanto la velocidad como la distancia (rango) se reducen notablemente. En

este sentido les ocurre lo mismo que a las redes Wi-Fi. Para una transmisión a distancias mayores (en teoría puede llegar hasta los 50Km) es necesario que las antenas tengan una línea de visión directa (LOS). [115]

1.7.2.2.8 WIFI FRENTE A WIMAX

WiMAX es al estándar 802.16 lo que Wi-Fi al 802.11. WiMAX no ha sido diseñado para ser competidor de Wi-Fi sino más bien para complementar a Wi-Fi en aquellas carencias que éste presenta.

La primera norma inalámbrica (802.11) fue desarrollada como una alternativa al cableado estructurado de redes LAN. Esta norma fue diseñada para ofrecer "conexión Ethernet "inalámbrica".

La certificación Wi-Fi fue elaborada para ofrecer una garantía de interoperabilidad entre productos 802.11 de diferentes fabricantes. Para entender mejor las aplicaciones para la cuales Wi-Fi fue diseñado, hay que imaginar una red Ethernet dentro de una oficina durante los años noventa.

El requerimiento era una red dentro de una oficina. Wi-Fi fue diseñado para ambientes inalámbricos internos y las capacidades sin línea de vista (NLOS) son posibles únicamente para unos pocos metros. A pesar de este diseño y de todas las limitaciones, había muchos proveedores de Internet (ISP) que implementaban radios Wi-Fi para servicio de Última Milla. Debido al diseño de Wi-Fi, los servicios en estas redes eran bastante limitados.

En los últimos años hemos visto mucho desarrollo en Wi-Fi y Ethernet para adaptarse a los cambios en las redes de datos. Esto incluye mejor seguridad (encriptación), redes virtuales (VLAN), y soporte básico para servicios de voz (QoS).

En conclusión, Wi-Fi fue diseñado para redes locales (LAN) para distancias cortas dentro de una oficina.

[115] ALMALASI, 2009.

WiMAX está basado en la norma 802.16. Esta norma fue diseñada específicamente como una solución de Última Milla, y enfocada en los requerimientos para prestar servicio a nivel comercial. Para empezar, su diseño contempla la necesidad de varios protocolos de servicio.

Una conexión WiMAX soporta servicios paquetizados como IP y voz sobre IP (VoIP), como también servicios conmutados (TDM), E1/T1 y voz tradicional (clase-5); también soporta interconexiones de ATM y Frame Relay. WiMAX facilita varios niveles de servicio (MIR/CIR) para poder dar diferentes velocidades de datos dependiendo del contrato con el suscriptor.

Un radio WiMAX tiene la capacidad de entregar varios canales de servicio desde la misma conexión física. Esto permite que múltiples suscriptores estén conectados al mismo radio (CPE); cada uno con una conexión privada con el protocolo y nivel de servicio que éste requiera. Esta solución garantiza tener múltiples suscriptores que se encuentran en un mismo edificio (MDU).

Adicionalmente a los servicios que WiMAX puede ofrecer, la tecnología de transmisión OFDM es una solución robusta para operar en condiciones donde no hay línea de vista (NLOS) a distancias de varios kilómetros. Esto es un requerimiento obligatorio para un caso de negocios de servicio inalámbrico en la última milla.

WiMAX y Wi-Fi son soluciones complementarias para dos aplicaciones bastante diferentes. WiMAX fue diseñado para redes metropolitanas (MAN), también conocido como "última milla". Wi-Fi fue diseñada para redes locales (LAN), también conocido como "Distribución en Sitio".[116]

1.7.2.2.9 RADIO FRECUENCIA

Las Redes Inalámbricas de Radiofrecuencia, la FCC permitió la operación sin licencia de dispositivos que utilizan 1Watt de energía o menos, en tres bandas de frecuencia: 902

[116] WIMAXTECH, 2009.

a 928MHz, 2,400 a 2,483.5MHz y 5,725 a 5,850Mhz. Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera.

Para minimizar la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada spread - spectrummodulation, la cual tiene potencia de transmisión máxima de 1Watt. Deberá ser utilizada en la banda ISM. Esta técnica ha sido utilizada en aplicaciones militares.

La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable.

La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente:

La secuencia directa: En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

El salto de frecuencia: Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia.

Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8Mhz que son utilizadas por hornos de Microondas. [117]

1.7.2.3 ANTENAS

Las antenas son un componente muy importante de los sistemas de comunicación. Las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física.

Definición.- Una antena es un dispositivo utilizado para transformar una señal de RF que viaja en un conductor, en una onda electromagnética en el espacio abierto.

Las antenas exhiben una propiedad conocida como reciprocidad, lo cual significa que una antena va a mantener las mismas características sin importar si está transmitiendo o recibiendo. La mayoría de las antenas son dispositivos resonantes, que operan eficientemente sólo en una banda de frecuencia relativamente baja.

Una antena debe ser sintonizada en la misma banda que el sistema de radio al que está conectada, para no afectar la recepción y transmisión. Cuando se alimenta la antena con una señal, emitirá radiación distribuida en el espacio de cierta forma. La representación gráfica de la distribución relativa de la potencia radiada en el espacio se llama diagrama o patrón de radiación.

Antes de hablar de antenas específicas, hay algunos términos que deben ser definidos y explicados:

Impedancia de entrada.- Para una transferencia de energía eficiente, la **impedancia** del radio, la antena, y el cable de transmisión que las conecta debe ser la misma. Las antenas y sus líneas de transmisión generalmente están diseñadas para una impedancia de 50Ω. Si la antena tiene una impedancia diferente a 50Ω, hay una desadaptación y se necesita

[117] Hacker Friendly, 2008.

un circuito de acoplamiento de impedancia. Cuando alguno de estos componentes no tiene la misma impedancia, la eficiencia de transmisión se ve afectada.

Pérdida de retorno.- Es otra forma de expresar la desadaptación. Es una medida logarítmica expresada en dB, que compara la potencia reflejada por la antena con la potencia con la cual la alimentamos desde la línea de transmisión. La relación entre SWR (*Standing Wave Ratio*—Razón de Onda Estacionaria) y la pérdida de retorno es la siguiente:

Pérdida de Retorno (en dB) = 20log10 SWR/SWR-1

Aunque siempre existe cierta cantidad de energía que va a ser reflejada hacia el sistema, una pérdida de retorno elevada implica un funcionamiento inaceptable de la antena.

Ancho de banda.- 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.

Los diferentes tipos de antenas tienen variadas limitaciones de ancho de banda.
EL ancho de banda viene definido por la relación que existe entre los paquetes transmitidos y el tiempo de duración de este proceso.

Ancho de banda = PT/t.

Eficiencia de la antena.- Esta eficiencia nos dice que tanto por uno de la potencia que le llega a la antena (Pet) es realmente radiada.

$$nt = \frac{Pt}{Pt + Pp} = \frac{Rt}{Rt + Rp}$$

Siendo nt (la n generalmente representada por la letra griega 'eta' y el subíndice t) la eficiencia de la antena en transmisión

Pt: Potencia Transmitida

Pp: Potencia de perdidas

Rt: Resistencia de Radiación (representa la energía que se irradia al espacio libre)

Rp: Resistencia de pérdidas (son debidas al paso de la corriente de un conductor no ideal que es con el que está construido la antena y otros)

Densidad de potencia de una antena.- Es la potencia transmitida por unidad de superficie. El denominador es el área de una esfera de radio d. La densidad de potencia nos indica cuantos Watios tenemos en una superficie de un metro cuadrado a una distancia d (en metros) de la antena.

La antena isotrópica radia la misma potencia en todas las direcciones, lo cual hace que Siso = cte para todas las direcciones. Sin embargo, la densidad de potencia de una antena cualquiera no será constante y dependerá para cada dirección.

Densidad de potencia de una antena isotrópica:

$$Siso = \frac{Pt}{4 \cdot pi \cdot d^2} \quad [W/m^2]$$

Pt= Potencia Transmitida

d= Distancia a la antena.

Directividad.- Es la habilidad de una antena de transmitir enfocando la energía en una dirección particular, o de recibirla de una dirección particular. Si un enlace inalámbrico utiliza ubicaciones fijas para ambos extremos, es posible utilizar la directividad de la antena para concentrar la transmisión de la radiación en la dirección deseada.

En una aplicación móvil, donde la antena no está fijada a un punto, es imposible predecir dónde va a estar, y por lo tanto la antena debería radiar en todas las direcciones del plano horizontal. En estas aplicaciones se utiliza una antena omnidireccional.

Representa la relación entre la densidad de potencia radiada por nuestra antena (S) respecto de lo que radiaría la antena isotrópica.

$$D(T,P) = \frac{S(T,P)}{Siso} = \frac{S(T,P)}{Pt/4 \cdot pi \cdot d^2}$$

Donde: T y P son las componentes 'tita' y 'phi' de las coordenadas esféricas. Tita es el ángulo que se toma con respecto de la referencia vertical (Z) y phi es el ángulo que se toma respecto de la referencia horizontal (X).

La directividad es cuanta potencia más o menos radia esa antena respecto de la antena isotrópica. Este parámetro depende de la dirección que se tome, ya que como hemos dicho una antena generalmente no radia por igual en todas las direcciones. Al establecer un radioenlace buscaremos que las antenas estén apuntadas de tal forma que la ganancia directiva sea la máxima en la dirección del receptor, esta ganancia directiva máxima es lo que se llama Directividad:

$$Dmax = \frac{Smax}{Siso}$$

También puede decirse que la directividad es el cociente entre la densidad de potencia del lóbulo principal y la densidad de potencia que se tendría con una antena isotrópica. Dmax de la antena isotrópica vale 1.

Ganancia de Potencia - Ganancia de la antena.- Idealmente una antena debería radiar toda la potencia que le entrega el generador, pero debido a que las antenas están construidas con materiales conductores reales, materiales que no tienen una conductividad infinita, se produce un calentamiento de la antena que supone una

pérdida de potencia (hay una potencia disipada en forma de calor en la antena). La ganancia de potencia de una antena es la ganancia directiva teniendo en cuenta estas pérdidas.

$G(T,P)= nt \cdot D(T,P)$

La ganancia de una antena directiva es la ganancia de potencia que tiene la antena en la dirección de máxima radiación.

$Gmax = nt \cdot Dmax$
Gmax= Ganancia de la antena
nt= eficiencia de la antena (valores entre 0 y 1)
Dmax= Directividad de la antena

En la práctica cuando se habla de ganancia (G) de una antena se suele hablar de la ganancia máxima de potencia (Gmax) y se le suele denominar simplemente ganancia. La diferencia entre la ganancia directiva y la ganancia de potencia es que la ganancia de potencia incluye ya las pérdidas de la antena.[118]

La ganancia no es una cantidad que pueda ser definida en términos de una cantidad física como vatios u ohmios: es un cociente sin dimensión. La ganancia se expresa con referencia a una antena estándar. Las dos referencias más comunes son la antena isotrópica y la antena dipolo resonante de media longitud de onda.

La antena isotrópica irradia en todas direcciones con la misma intensidad. En la realidad esta antena no existe, pero provee un patrón teórico útil y sencillo con el que se puede comparar las antenas reales. Cualquier antena real va a irradiar más energía en algunas direcciones que en otras. Puesto que las antenas no crean energía, la potencia total irradiada es la misma que una antena isotrópica. Una ganancia de antena de 3dB comparada con una isotrópica debería ser escrita como 3dBi. La antena dipolo resonante de media longitud de onda puede ser un estándar útil a la hora de compararlo con otras antenas a una frecuencia, o sobre una banda estrecha de frecuencias. La ganancia de una

[118] Merlos, 2009.

antena comparada con un dipolo debería ser escrita como 3dBd. Entonces cuando hay un valor en dBi, comparado con el valor isotrópico, o bien un dBd si se lo ha hecho sobre el dipolo estándar se puede utilizar la siguiente formula y comparar ambos valores

dBd + 2.15 = dBi

Y si al contrario el valor nos lo dan en dBi, habrá que restarle 2.15, para saber su valor en dBd. [119]

Diagramas o Patrones de Radiación.- Los patrones o diagramas de radiación describen la intensidad relativa del campo radiado en varias direcciones desde la antena a una distancia constante.

El patrón de radiación es también de recepción, porque describe las propiedades de recepción de la antena. El patrón de radiación es tridimensional, pero generalmente las mediciones de los mismos son una porción bidimensional del patrón, en el plano horizontal o vertical. Estas mediciones son presentadas en coordenadas rectangulares, o en coordenadas polares.

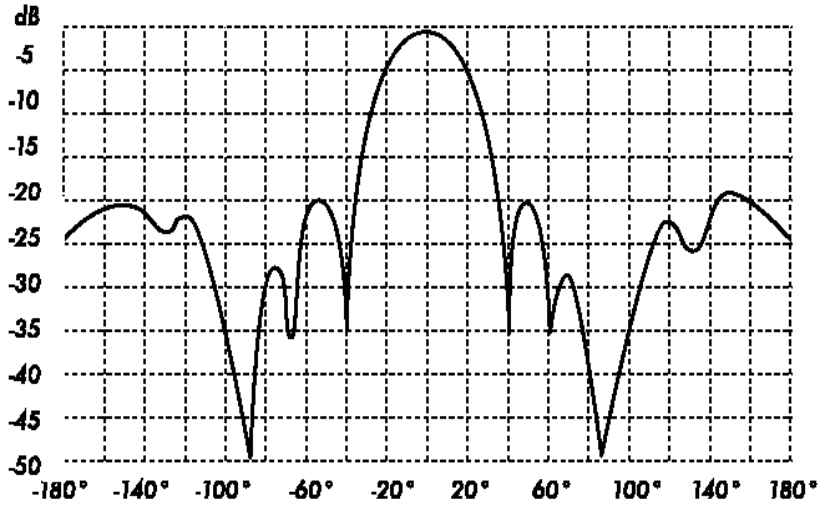


Fig. 1.63 Radiación de una antena Yagi en coordenadas rectangulares

Fuente: Friendly LLC, Hacker, 2008

[119] W3, 2009.

Polarización de la antena.- La polarización de una antena se refiere sólo a la orientación del campo eléctrico radiado desde ésta. Una antena puede polarizarse en forma lineal (por lo regular, polarizada horizontalmente o verticalmente, suponiendo que los elementos de la antena se encuentran dentro de un plano horizontal o vertical), en forma elíptica, o circular. Si una antena irradia una onda electromagnética polarizada verticalmente, la antena se define como polarizada verticalmente; si la antena irradia una onda electromagnética polarizada horizontalmente, se dice que la antena está polarizada horizontalmente; si el campo eléctrico gira en un patrón elíptico, está polarizada elípticamente; y si el campo eléctrico gira en un patrón circular, está polarizada circularmente.[120]

Desadaptación de polarización.- Para transferir la máxima potencia entre una antena transmisora y una receptora, ambas antenas deben tener la misma orientación espacial, el mismo sentido de polarización y el mismo coeficiente axial.

Cuando las antenas no están alineadas o no tienen la misma polarización, habrá una reducción en la transferencia de potencia entre ambas antenas. Esto va a reducir la eficiencia global y las prestaciones del sistema. Cuando las antenas transmisora y receptora están polarizadas linealmente, una desalineación física entre ellas va a resultar en una pérdida por desadaptación de polarización.

Resumiendo, cuanto más grande la desadaptación de polarización entre una antena transmisora y una receptora, más grande la pérdida aparente. En el mundo real, la pérdida debida a una desadaptación en polarización de 90° es bastante grande pero no infinita. La polarización puede aprovecharse en un enlace punto a punto. [121]

Ancho del haz de la antena.- El ancho del haz de la antena es solo la separación angular entre los dos puntos de media potencia (-3 dB) en el lóbulo principal del patrón de radiación del plano de la antena, por lo general tomado de uno de los planos "principales".[122]

[120] Berdiñas, 2009.
[121] Friendly, 2008.
[122] Berdinas, 2009.

1.7.2.3.1 TIPOS DE ANTENAS

Una clasificación de las antenas puede basarse en:

- **Frecuencia y tamaño.-** Las antenas utilizadas para HF son diferentes de las antenas utilizadas para VHF, las cuales son diferentes de las antenas para microondas. La longitud de onda es diferente a diferentes frecuencias, por lo tanto las antenas deben ser diferentes en tamaño para radiar señales a la correcta longitud de onda. Las antenas que trabajan en el rango de microondas, especialmente en las frecuencias de los 2,4GHz y 5GHz. A los 2400MHz la longitud de onda es 12,5 cm, mientras que a los 5000MHz es de 6 cm.

- **Directividad.-** Las antenas pueden ser omnidireccionales, sectoriales o directivas.

- **Antenas omnidireccionales.-** Las cuales dan cobertura con un diagrama de radiación teórico de una esfera, aunque en la práctica es un diagrama de radiación circular (360º), ya que una antena no puede emitir en su vertical. Se supone que dan servicio por igual independientemente de su colocación, pero debido a que las frecuencias en las que están trabajando son próximas a microondas, los diagramas no son circulares, son óvalos.[123]

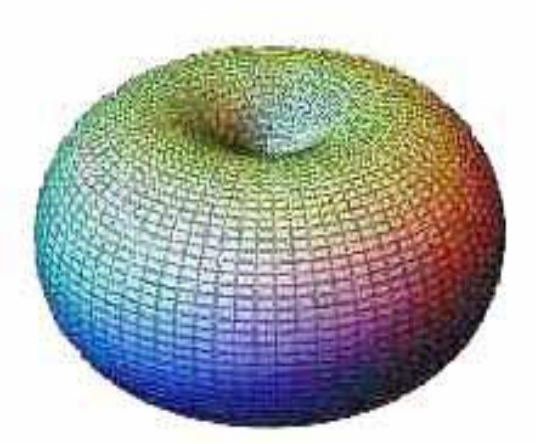


Fig. 1.64 Ovulo de Radiación de una antena omnidireccional

Fuente: Ignacio Pérez, 2007

[123] Pérez, 2007.

Baja ganancia con 8,12 y 15dBi, Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales. El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Los tipos más populares de antenas omnidireccionales son los dipolos y las de plano de tierra.

Fig. 1.65 Antena omnidireccional
Fuente: Carolina Betancourth, 2009.

Antenas Sectoriales

Irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados.

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional.

Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.[124]

Antenas Direccionales

Solo emiten/reciben con un ancho de haz definido por la construcción de la antena.[125]

Su ancho del haz es mucho más angosto que en las antenas sectoriales. Estas antenas están destinadas a enlaces punto a punto y son ideales para los enlaces Bridge point to point, point to multipoint, tienen la ganancia más alta y por lo tanto se utilizan para enlaces a larga distancia, son utilizados para los equipos WLAN, pudiendo llegar hasta 37 o 39 dBi.

Tipos de antenas directivas son las Yagi, las biquad, las de bocina, las helicoidales, las antenas patch, etc.

Los esquemas de las antenas son:

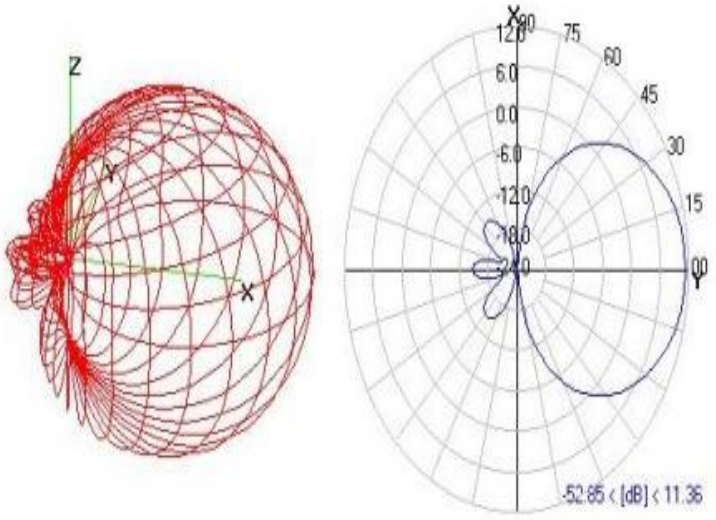


Fig. 1.66 Esquema de las Antenas Direccionales

Fuente: Compostela Wireless, 2009

[124] Trucoswindows.Net, 2009.
[125] Pérez, 2007.

Antenas Bi-Quad

La antena Bi-Quad, pertenece al grupo de las antenas sectoriales y directivas, es decir, concentra su efectividad en un sentido y dirección principalmente, el lóbulo principal o delantero.

Esta antena está conformada por un arreglo de 2 cuadros de algún medio conductor de lado λ/4, o sea, aproximadamente 30.5mm, que en sus intersecciones conectan a la línea transmisora, generalmente a través de un conector N.

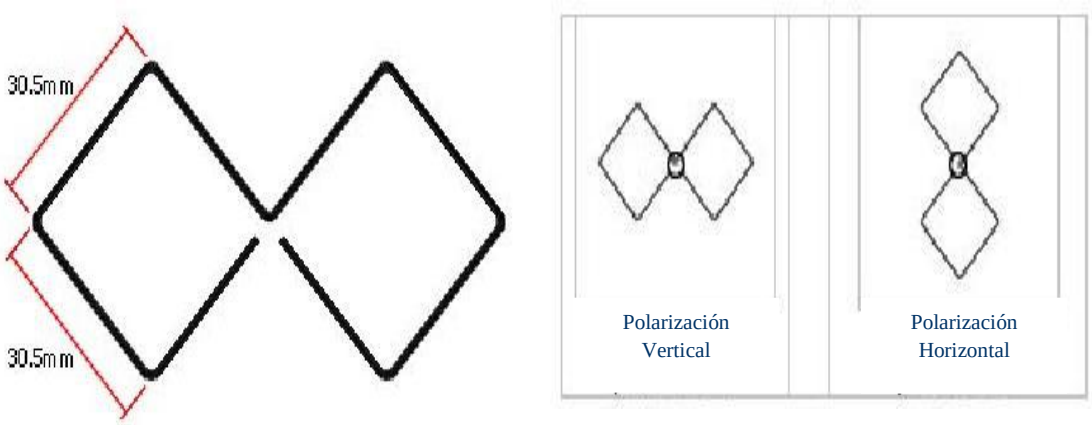


Fig. 1.67 Dimensión del Bi-Quad y polarización de las Antenas Direccionales
Fuente: Compostela Wireless, 2009

Como es posible apreciar en la grafica, la polaridad de esta antena está dada por su geometría, siendo esta opuesta a su posición aparente, al estar la antena físicamente horizontal, su polaridad será vertical y viceversa.

Variantes del Biquad

El modelo más común de antena Bi-Quad es el construido en base a un alambre de cobre doblado en las dimensiones antes mencionadas, conectado directamente al cable conductor, y que posee además un reflector también de cobre.

Esta antena logra ganancias del orden de los 11 o 12 dBi.

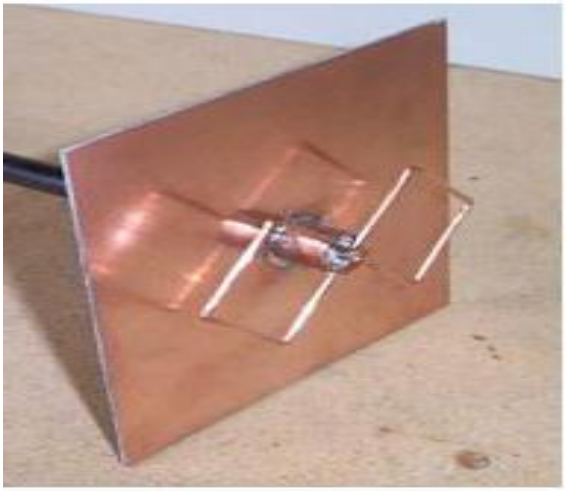


Fig. 1.68 Antena Bi-Quad
Fuente: Compostela Wireless, 2009

Otra variación a esta misma antena es la doble Bi-Quad, que posee la misma construcción, pero le son adicionados dos cuadros más de cobre de igual medida.

El resultado de esta modificación es un aumento en la ganancia de la antena del orden de 2 dB.

Una tercera variación de esta antena, esta dado por la confección del cuadro de cobre directamente sobre un conector N, esto simplifica la construcción y al eliminar interconexiones y cable, podría reducir perdidas.

Sustento Teórico

Ya se ha visto las distintas formas en que se construye una antena Bi-Quad, las características de su lóbulo, su ganancia, etc. Pero ¿cómo funciona?

El elemento radiante es un par de vueltas de conductor, que en su perímetro recorre una longitud de onda λ cada uno.

Es necesario imaginar una onda viajando a través de cada vuelta siendo la cresta de la onda indicada con (+), el valle con un (-), y el punto de cruce con un ‘0’.

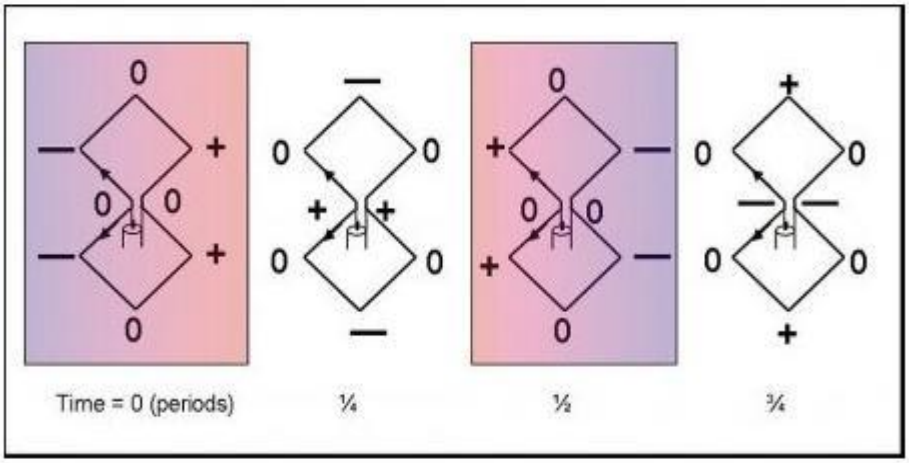


Fig. 1.69 Sustento teórico de la Antena Bi-Quad

Fuente: Compostela Wireless, 2009

A medida que la onda atraviesa el circuito la señal parece cambiar de lado a lado.

Con respecto a la ubicación del reflector, existen indicaciones distintas según el fabricante, esto al parecer se debería a que con el reflector a una distancia equivalente a λ/8, o sea a 15mm se lograría el máximo bandwidth y menor ROE (resultado experimental); mientras que la teoría de antenas nos dice que todo reflector debe estar ubicado a una distancia equivalente a λ/4 (o un múltiplo impar) lo que en nuestro caso sería del orden de los 30mm, esto para que las ondas entren en fase.

Con respecto al cálculo teórico de la ganancia de esta antena, es posible relativilizarlo a un dipolo de media onda, esto se logra mediante el análisis de su geometría, siendo cada lóbulo el equivalente a una antena dipolo de ½ onda de 3dB.

Entonces:

2 x 3 = 3dB + 3dB = 6dB

Más el reflector = 6dB

Total = 12dB

Menos Perdidas (conectores, etc) = 10dB

Doble Bi-Quad

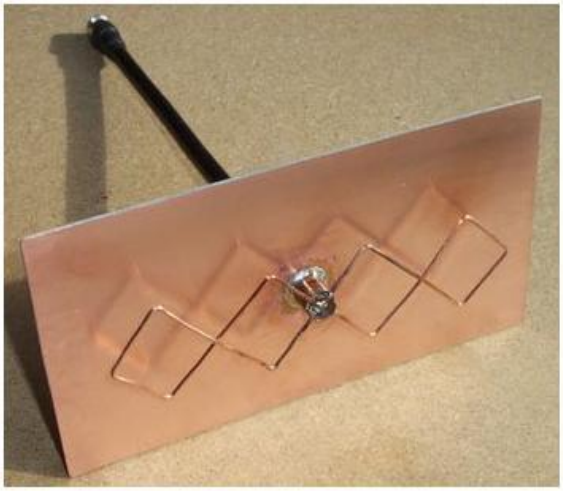


Fig. 1.70 Antena de doble Bi-Quad
Fuente: Compostela Wireless, 2009

En vista de toda la información existente con respecto a las antenas Bi-Quad, sus características favorables, y el ser una antena 'probada' por muchos usuarios, genera la motivación para hacer esta antena.

El copiar un modelo existente, con planos de fabricación, no presenta ninguna dificultad, ni tampoco una mejora a lo existente, tampoco brinda la posibilidad real de aprender.

A partir de estos hechos nace la idea de resolver algunas de las problemáticas que presenta esta antena. La principal es debida a lo exacto de las mediciones en esta longitud de onda, al tratarse de medidas en milímetros; como se ha visto las construcciones son principalmente en alambre de cobre que es doblado con la mayor precisión posible de sus ángulos y largos.

La idea es generar una geometría rigurosa, objetivo no siempre cumplido dado los materiales, y el resultado tampoco es durable en el tiempo dado la flexibilidad del material.[126]

- **Construcción física.-** Las antenas pueden construirse de muchas formas diferentes, desde simples mallas, platos parabólicos, o latas de café. Cuando consideramos antenas adecuadas para el uso en WLAN de 2,4GHz.

- **Aplicaciones.-** Los puntos de acceso tienden a hacer redes punto a multipunto, mientras que los enlaces remotos son punto a punto. Esto implica diferentes tipos de antenas para el propósito. Los nodos utilizados para accesos multipunto pueden utilizar tantas antenas omni las cuales irradian igualmente en todas direcciones, como antenas sectoriales que se enfocan en un área limitada. En el caso de los enlaces punto a punto, las antenas se usan para conectar dos lugares.

1.7.2.3.2 LÍNEA VISUAL O LÍNEA DE VISTA

El término línea visual, a menudo abreviada como LOS (por su sigla en inglés, Line of Sight), es fácil de comprender cuando hablamos acerca de la luz visible: si podemos ver un punto B desde un punto A donde estamos, tenemos línea visual. Dibuje simplemente una línea desde A a B, y si no hay nada en el camino, tenemos línea visual.

Las cosas se ponen un poco más complicadas cuando estamos tratando con microondas. Recuerde que la mayoría de las características de propagación de las ondas electromagnéticas son proporcionales a la longitud de onda. Este es el caso del ensanchamiento de las ondas a medida que avanzan. La luz tiene una longitud de onda de aproximadamente 0,5 micrómetros, las microondas usadas en las redes inalámbricas tienen una longitud de onda de unos pocos centímetros. Por consiguiente, los haces de microondas son más anchos, necesitan más espacio.

[126] COMPOSTELA, 2009.

Note que los haces de luz visibles también se ensanchan, y si los dejamos viajar lo suficiente, podemos ver los resultados a pesar de su pequeña longitud de onda. Cuando apuntamos un láser bien enfocado a la luna, el haz se extenderá abarcando más de 100 metros de radio cuando alcance su superficie.

La línea visual que necesitamos para tener una conexión inalámbrica óptima desde A hasta B es más que simplemente una línea delgada –su forma es más bien la de un cigarro, una elipse. Su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

1.7.2.3.3 PERTURBACIONES EN LA TRANSMISIÓN

Al ser transmitida la señal suceden eventos no deseados que alteran la calidad de la señal. Entre estos problemas los más difíciles de tratar o resolver son el ruido, la distorsión y la interferencia debido a que éstos afectan la forma de la señal

La atenuación por sí sola no es un gran problema, es suficiente amplificar la señal, pero el problema radica en que la señal generalmente además de ir atenuada también va contaminada ya sea con ruido, distorsión o interferencia y éstos se amplifican junto con la señal.

Perturbaciones:

- Atenuación
- Distorsión de retardo
- Ruido

Atenuación

Consiste en el debilitamiento o pérdida de amplitud de la señal recibida frente a la transmitida. A partir de una determinada distancia, la señal recibida es tan débil que no se puede reconocer mensaje alguno. La solución a este problema la encontramos en el uso de repetidores (caso de señales digitales) o amplificadores (señales continuas).

Problemas:

- La señal recibida debe tener la suficiente energía para que la electrónica en el receptor pueda detectar e interpretar la señal
- La señal debe recibirse con un nivel mayor que el ruido
- La atenuación varía en función de la frecuencia, lo que provoca que la señal recibida esté distorsionada

Soluciones:

- Amplificadores o repetidores: incrementan la energía de la señal.
- Ecualizadores: amplifican de forma diferente cada frecuencia evitan la distorsión de la señal

La Distorsión por Atenuación

La atenuación al ser una función de la distancia y la frecuencia produce que señales diferentes ocasionen distorsiones diferentes .Para compensar esta diferente atenuación a distintas frecuencias, los amplificadores pueden incorporar una etapa denominada ecualizador.[127]

Distorsión por Eventos Metereológicos

Es cuando ocurren eventos metereológicos como lluvia, nieve etc. Los cuales distorsionan o anulan la transmisión de la señal, son más frecuentes en las transmisiones satelitales.

Distorsión de Retardo

- Fenómeno característico de los medios guiados.
- Se produce por la diferente velocidad de propagación de las distintas componentes frecuenciales que forman la señal.

[127] Atenea, 2007.

- Cada armónico es recibido en un instante de tiempo diferente la señal reconstruida sufre una distorsión respecto a la señal original.[128]

Ruido

Son señales eléctricas que muestran un comportamiento aleatorio e impredecible y pueden originarse dentro y fuera del sistema de comunicación. Afecta generalmente a la señal portadora de la información, ocultándola o eliminándola total o parcialmente.

Tipos de ruido:

- **Ruido Endógeno:** Este ruido es producido dentro del propio sistema de comunicación.
- **Ruido Exógeno:** Contrario al ruido endógeno, este ruido es producido fuera del sistema de comunicación.
- **Ruido Blanco O Gaussiano:** Este tipo de ruido se caracteriza porque su energía o densidad es cortante sobre todas las frecuencias de la señal. Es común percibirlo cuando en la frecuencia FM no hay señal.
- **Ruido térmico**: Debido a la agitación térmica de electrones dentro del conductor.
- **Ruido de intermodulación**: Cuando distintas frecuencias comparten el mismo medio de transmisión.
- **Ruido impulsivo:** Este ruido no es constante sólo aparece en intervalos irregulares de tiempo, con picos de corta duración y gran amplitud.[129]

Diafonía

La Diafonía (Crosstalk): Es un fenómeno que todos hemos experimentado en las comunicaciones telefónicas. Consiste en la interferencia de un canal (o cable)

[128] Docente. UCOL, 2009.
[129] Potosí, 2009.

próximo con el nuestro, esto produce una señal que es la suma de la señal transmitida y otra señal externa atenuada que aparece de fondo. En una conversación telefónica esto se escucha como una segunda conversación que se oye de fondo mezclada con la nuestra.

Diafonía Next: Near End Cross Talk. Cerca de interferencia, es la medida del ruido que se induce eléctricamente a partir de un par, en el cable sobre otro par, o de los pares. Si este ruido llega a ser excesivo, conducirá para señalar pérdida o aún la interrupción total de la comunicación. Pero la cosa más importante es mantener las torceduras del par tan apretadas como sea posible hasta el punto de la terminación. La señal en parte regresa al transmisor.[130]

1.7.2.3.4 ZONA DE FRESNEL

La teoría exacta de las zonas de Fresnel es algo complicada. Sin embargo, el concepto es fácilmente entendible: sabemos, por el principio de Huygens, que por cada punto de un frente de onda comienzan nuevas ondas circulares. Sabemos que los haces de microondas se ensanchan.

También sabemos que las ondas de una frecuencia pueden interferir unas con otras. La teoría de zona de Fresnel simplemente examina a la línea desde A hasta B y luego el espacio alrededor de esa línea que contribuye a lo que está llegando al punto B. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas.

Consecuentemente, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos. Siempre que el desplazamiento de fase es de una longitud de onda completa, se obtiene una interferencia constructiva: las señales se suman óptimamente.

Tomando este enfoque, y haciendo los cálculos, nos encontramos con que hay zonas anulares alrededor de la línea directa de A a B que contribuyen a la señal llega al punto

[130] Fonseca, 2009.

B. Tenga en cuenta que existen muchas zonas de Fresnel, pero a nosotros nos interesa principalmente la zona 1. Si esta fuera bloqueada por un obstáculo, como un árbol o un edificio, la señal que llegue al destino lejano será atenuada.

Entonces, cuando planeamos enlaces inalámbricos, debemos asegurarnos de que esta zona va a estar libre de obstáculos. En la práctica, en redes inalámbricas nos conformamos con que al menos el 60% de la primera zona de Fresnel esté libre.[131]

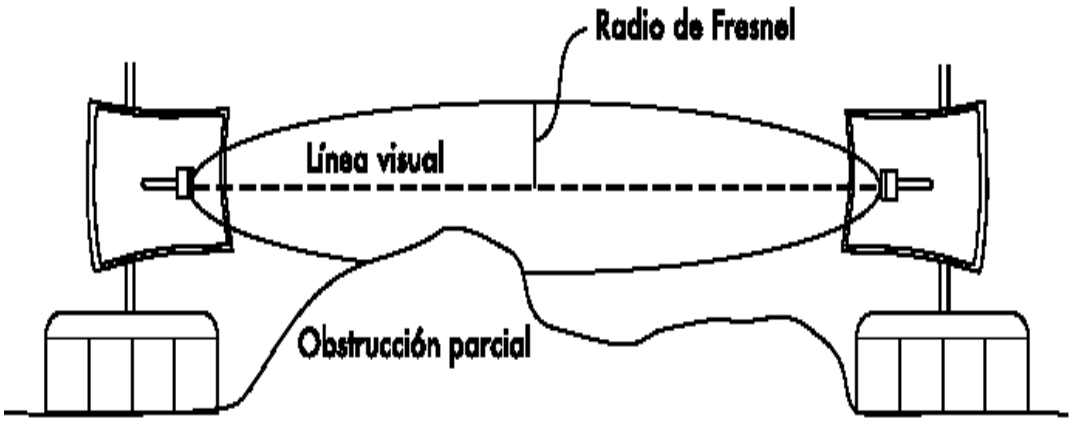


Fig. 1.71 Línea visual o línea de vista
Fuente: Friendly LLC, Hacker. 2008

Teoria De Calculo

La Zona de Fresnel es la altura ideal (radio) en la cual se deben posicionar el NODO y CPE para poder realizar un enlace confiable dependiendo de la frecuencia y la distancia:

La constante de Fresnel establece lo siguiente:

$$r = 17.32\sqrt{\frac{D}{4f}}$$

- r = radio en metros

[131] Hacker Friendly LLC, 2008.

- D = distancia total del enlace en kilómetros
- f = frecuencia del enlace en gigahertz (2.4, 5.8Ghz, etc)

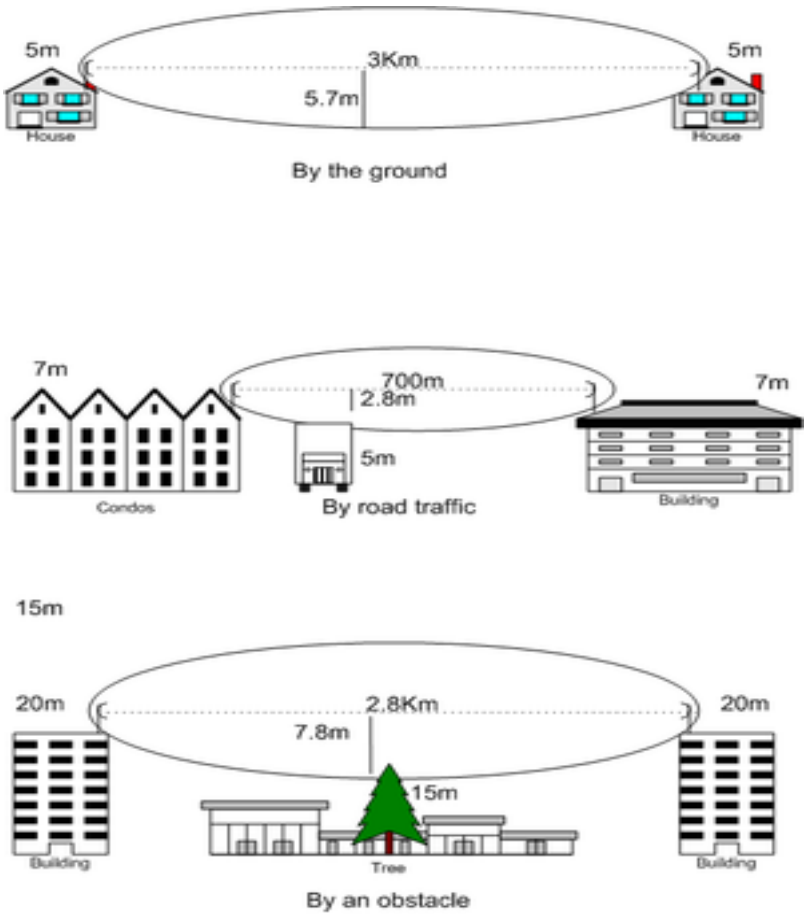


Fig. 1.72 Zonas de Fresnel para 3, 0.7 y 2.8 km

Fuente: Tamahome, 2008

Ejemplos

De esta manera, para un simple enlace de 3km, aplicando la fórmula, necesitaremos un radio de 9.68mts, por lo que el NODO y el CPE se deberían encontrar al menos a 10mts de altura.

En el caso de que la altura del nodo sea significativamente mayor (40mts por ejemplo) necesitaremos menor altura en el CPE para poder realizar el radioenlace.

En el ejemplo de la imagen anterior, notamos obstáculos de por medio, por lo que el radio de 9.68mts calculado será a partir del obstáculo más alto de por medio. Ej.: Si en nuestra línea de visión se encuentra un árbol de 5mts de altura, las distancias ideal para nuestro radioenlace será de 5mts + 9.68mts = 14.68mts.

Estos cálculos son todos para conexiones ideales, se estima que con respetar el radio de Fresnel en al menos un 66% se puede lograr un enlace estable. Convirtiendo los 9.68mts en 6.4mts y la altura con un obstáculo de 5mts de 14.68 en 9.7mts aprox.[132]

1.7.2.3.5 TRANSMISIÓN DE DATOS EN REDES INALÁMBRICAS

El Hombre siempre se ha comunicado, de una forma u otra. El proceso de la comunicación ha ido creciendo y mejorando los mecanismos utilizados hasta llegar a lo que hoy conocemos y utilizamos. Toda comunicación lleva implícita la transmisión de información de un punto a otro, pasando por una serie de procesos.

Una de las definiciones más comunes de transmisión de datos:

Parte de la transmisión de información que consiste en el movimiento de información codificada, de un punto a uno o más puntos, mediante señales eléctricas, ópticas, electro ópticas o electromagnéticas.

Los principales objetivos que debe satisfacer un sistema de transmisión de datos son:

- Reducir tiempo y esfuerzo.
- Aumentar la velocidad de entrega de la información.
- Reducir costos de operación.
- Aumentar la capacidad de las organizaciones a un costo incremental razonable.
- Aumentar la calidad y cantidad de la información.

Comunicaciones locales y remotas

Según la ubicación geográfica se puede hablar de dos tipos de transmisión de datos:

[132] PHPBB.TAMAX, 2009.

Transmisión de datos local.- También denominada "en planta". Las distancias son pequeñas. En este caso es la propia organización (empresa, universidad, factoría, etc.) la que construye las líneas de comunicaciones.

Ej. Un computador central al que se quiere conectar varias terminales en distintos puntos de un edificio.

Transmisión de datos remota.- La distancia entre los equipos que se quieren comunicar es mucho mayor. Es necesario acceder a las líneas de telecomunicaciones para que se realice. Normalmente se accede a las líneas proporcionadas por el servicio telefónico.

Componentes de un Sistema de Transmisión.- Un sistema de comunicación de datos tiene como objetivo el transmitir información desde una fuente a un destinatario a través de una canal.

El esquema básico con el que podemos representar este concepto es:

- **El emisor o transmisor.-** Debe convertir la señal a un formato que sea reconocible por el canal.
- **El canal.-** Conecta al emisor (E) y receptor (R) y puede ser cualquier medio de transmisión (fibra óptica, cable coaxial, aire, etc.).
- **El receptor.-** Acepta la señal del canal y la procesa para permitir que el usuario final la comprenda.[133]

1.7.2.3.6 TIPOS DE TRANSMISIÓN

En estas redes, el medio físico que utilizamos para la comunicación es obviamente la energía electromagnética, sea que deba llegar hasta una oficina en un edificio o extenderse a lo largo de muchos kilómetros, las redes inalámbricas se organizan naturalmente en estas tres configuraciones lógicas: Transmisión punto a punto, punto a

[133] Pelliza, 2009.

multipunto, y nubes multipunto a multipunto. Si bien las diferentes partes de su red pueden aprovechar las tres configuraciones, los enlaces individuales van a estar dentro de una de esas topologías.

1.7.2.3.6.1 Punto a punto

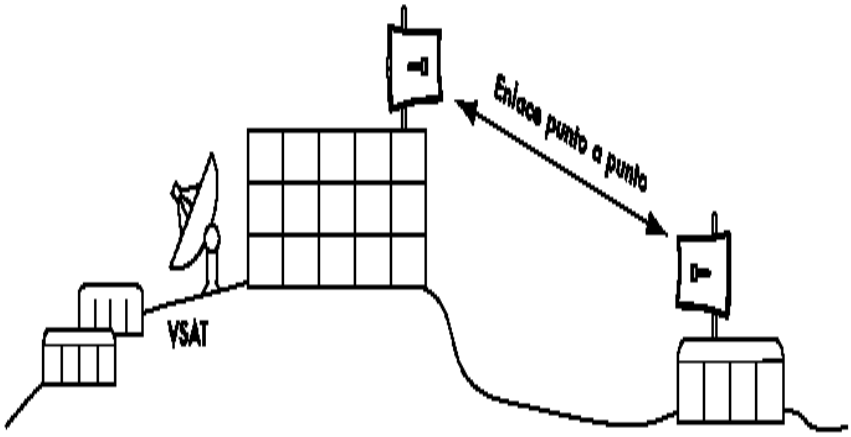


Fig. 1.73 Enlace Punto a Punto
Fuente: Friendly LLC, Hacker. 2008.

Los enlaces punto a punto generalmente se usan para conectarse a internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a internet, mientras que el otro utiliza el enlace para acceder a ella.

Si el edificio principal tiene una visión libre de obstáculos al lugar remoto, una conexión punto a punto puede ser utilizada para unirlos. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto confiables de más de cien kilómetros.

Una vez hecha una conexión punto a punto, se pueden añadir otras para extender la red aún más. Mediante la instalación de otro enlace punto a punto al lugar alejado, se puede unir a la red otro nodo y compartir la conexión central a internet.

Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a internet. Ejemplo: si desea desplazarse hasta una estación meteorológica alejada, ubicada en lo alto de una colina, para recolectar los datos que ella toma. Podría conectar

el lugar con un enlace punto a punto, logrando la recolección y el monitoreo de datos en tiempo real, sin tener que ir hasta el lugar.

Las redes inalámbricas pueden proveer suficiente ancho de banda como para transmitir grandes cantidades de datos (incluyendo audio y video) entre dos puntos, aún en ausencia de conexión a internet.

1.7.2.3.6.2 Punto a multipunto

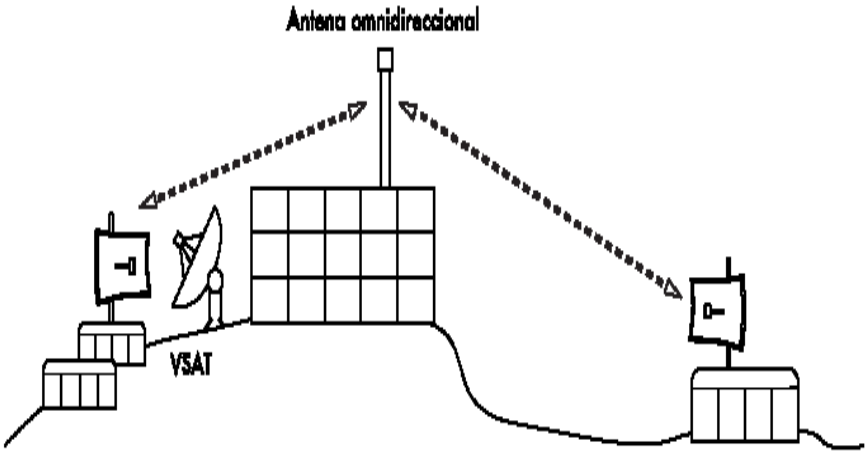


Fig. 1.74 Enlace Punto a Multipunto
Fuente: Friendly LLC, Hacker. 2008.

La siguiente red más común encontrada es la red punto a multipunto. Cada vez que tenemos varios nodos hablando con un punto de acceso central se está en presencia de una aplicación punto a multipunto.

El ejemplo típico de un trazado punto a multipunto es el uso de un punto de acceso (Access Point) inalámbrico que provee conexión a varias computadoras portátiles.

Las computadoras portátiles no se comunican directamente unas con otras, pero deben estar en el rango del punto de acceso para poder utilizar la red. Algunas limitaciones con el uso de enlaces punto a multipunto en distancias muy grandes.

1.7.2.3.6.3 Multipunto a multipunto

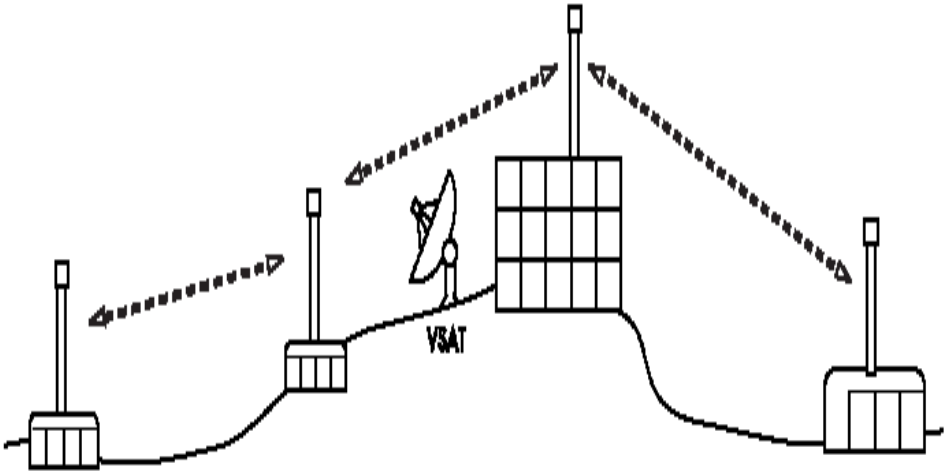


Fig. 1.75 Enlace Multipunto a Multipunto

Fuente: Friendly LLC, Hacker. 2008

El tercer tipo de diseño de red es el multipunto a multipunto, el cual también es denominado red ad-hoc o en malla (mesh). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí.

Las buenas implementaciones de redes mesh son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red mesh es tan sencillo como agregar más nodos. Si uno de los nodos en la "nube" tiene acceso a Internet, esa conexión puede ser compartida por todos los clientes.

Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento. La seguridad de esta red también es un tema importante, ya que todos los participantes pueden potencialmente transportar el tráfico de los demás.

La resolución de los problemas de las redes multipunto a multipunto tiende a ser complicada, debido al gran número de variables que cambian al moverse los nodos.

Las redes multipunto a multipunto generalmente no tienen la misma capacidad que las redes punto a punto, o las punto a multipunto, debido a la sobrecarga adicional de administrar el enrutamiento de la red y el uso más intensivo del espectro de radio.
Sin embargo, las redes mesh son útiles en muchas circunstancias.[134]

1.7.2.3.7 HOT SPOT (PUNTO CALIENTE)

Los hotspot Wi-Fi fueron propuestos en agosto de 1993 por Brett Stewart. Si bien Stewart no empleó el término "hotspot", sí se refirió al acceso público a redes LAN inalámbricas. El término "Hot-Spot" posiblemente haya sido propuesto por Nokia unos cinco años después de que Stewart proponga el concepto.

En la actualidad, los hotspot libres crecen exponencialmente, incluso extendiéndose a áreas metropolitanas de todo el mundo.

Definición.- Los Hot-spots son los lugares que ofrecen acceso Wi-Fi, que pueden ser aprovechados especialmente por dispositivos móviles como notebooks, PDAs, consolas, para acceder a internet.[135]

La mayoría de las redes Wi-Fi operan en el modo infraestructura: consisten en un punto de acceso en algún lugar (con un radio operando en el modo maestro), conectado a una línea DSL u otra red cableada de larga distancia.

En un “hot- spot” el punto de acceso generalmente actúa como una estación máster que distribuye el acceso a internet a sus clientes, que operan en el modo administrado. Esta topología es similar al servicio GSM de teléfonos móviles. Este punto de acceso generalmente está localizado en lugares con gran tráfico de público que proporciona servicios de red inalámbrica de banda ancha a visitantes móviles.[136]

> **Frecuencias.-** Una red de Wi-Fi usa un radio de frecuencia para comunicarse entre el dispositivo cliente y el punto de acceso, usa transmisores de doble banda (o doble sentido) que trabajan a 2.4 GHz (802.11b y/o 802.11g) o 5 GHz

[134] Hacker Friendly LLC, 2008.
[135] Diccionario Informático, 2009.
[136] Virusprot, 2003.

(802.11a). Por lo general, el alcance de la antena varía entre 30 y 300 metros de distancia entre el punto emisor y el receptor, dependiendo del tipo de antenas utilizadas y la potencia emitida. A pesar de esto, hay muchos factores que reducen el alcance efectivo, como las interferencias y las condiciones físicas de la sala o en caso de exteriores los elementos físicos.

Seguridad.- Debido a que la comunicación se establece mediante ondas electromagnéticas, la posibilidad de ser crackeados o que una persona extraña se apodere de la red, son bastantes. Sin embargo, existe la seguridad del tipo WEP y WPA para evitar el robo de datos. Independientemente de la seguridad aplicada en el enlace inalámbrico, en un Hot-Spot público carece de importancia el hacer una conexión cifrada. Si en un Hot-Spot se usa una red inalámbrica cifrada y el código de ésta es conocido, la facilidad para descifrar los datos es la misma.

En un Hot-Spot público se ha de aplicar una configuración peer-to-peer en todos los casos en capa 2 y evitar así el multicast o broadcast entre clientes. No se han de aplicar cifrados al enlace inalámbrico y se ha de posibilitar el uso de VPNs.[137]

[137] Wikipedia, 2009.

CAPITULO II

2.1. ANÁLISIS DEL ENLACE POR RADIO

De acuerdo a las entrevistas realizadas al Dr. Rimael Núñez, Director Del Departamento de Cultura de la UEB, Tecnólogo Antonio Tapia, Ayudante del Museo de la Escuela de Educación y Cultura Andina (EECA), y, al Dr. Henry Vallejo, Director del Departamento de Internet de la Universidad Estatal de Bolívar, se realizó el análisis del funcionamiento del sistema de conexión actual a internet tanto en la Casona Universitaria como en la Casa Regional de Bolívar, la cual se detalla a continuación:

a) Análisis de La Casa Regional de Bolívar

La Casa Regional de Bolívar, donde funcionan el departamento de Cultura y La Escuela de Cultura Andina de La Universidad Estatal de Bolívar, no disponen del servicio de Internet, ni una intranet. Las formas de comunicación son: por medio del teléfono analógico cuya estructura es dialup, del personal que labora en la EECA, cuentan con la colaboración del Sr. Eduardo Paredes, quien hace las veces de mensajero y conserje. Además cuentan con computadoras y líneas telefónicas que se detallan a continuación:

El departamento de Cultura, tiene la línea telefónica Nro. 2983-120 y tres computadoras: Una Pentium III, disco duro de 40 GHz y 256 MB de memoria RAM; dos Pentium IV, disco duro de 160 GHz y 512 MB de memoria RAM.

A sí mismo, La Escuela de Educación y Cultura Andina (EECA). Tiene la línea telefónica Nro. 2982-013 y tres computadoras. Una Pentium III que está deteriorada; Dos Pentium IV, disco duro de 160 GHz y 512 MB de memoria RAM.

b) Análisis de La Casona Universitaria

La Casona Universitaria dispone de una conexión a internet con banda ancha de 512 Mbps, a través de un MODEM de la Corporación Nacional de Telecomunicaciones. Posee una red interna con: un router marca TP-LINK el cual se encuentra en el departamento de Evaluación y Acreditación; dos switch marca 3COM de 24 puertos, uno en el laboratorio de Post-Grado y otro en la oficina que actualmente está ocupada por los voluntarios norteamericanos del Programa World Teach.

Las 29 computadoras están distribuidas de la siguiente manera: 11 computadoras en el laboratorio de computación de Post- Grado; 15 computadoras en las diferentes oficinas que laboran en la Casona Universitaria para sus actividades diarias, 3 computadoras portátiles para los voluntarios norteamericanos del Programa World Teach.

En la parte posterior de la Casona Universitaria se encuentra una torre prefabricada de 15 metros, en la cual están sujetas las antenas de: La Radio Universidad de Bolívar, la antena direccional marca Motorola CANOPY, la antena omnidireccional de 16 dBi y una caja hermética donde se encuentra un router configurado como Access Point marca Linksys WRT54-G.

La carencia de las tecnologías de comunicación e información y el no estar integrados a la red de datos de la Universidad Estatal de Bolívar. Han hecho que las labores cotidianas del departamento de Cultura y La Escuela de Cultura Andina de La UEB, se vean afectadas por no tener a su disposición las herramientas necesarias para un mejor desenvolvimiento en sus actividades encomendadas.

Además las formas de comunicación anteriormente descritas implican costos elevados y pérdida de tiempo en el envío de información.

Soluciones a la problemática planteada:

Es casi imposible realizar una conexión a través de cable (UTP o Fibra Óptica) desde la casona Universitaria a la Casa Regional de Bolívar (471 metros), ya que estos sitios se encuentran en el centro de la ciudad, implicando llevar la señal a través de los postes instalados por la empresa eléctrica o rompiendo calzada; en ambos casos, el cable debería estar protegido en una manguera PVC de ¾ pulgadas; además el cableado aéreo técnicamente no es recomendado, lo que incide en costos muy elevados, los trámites para conseguir los permisos en la Corporación Nacional de Electricidad S.A para la utilización de los postes o al Gobierno Municipal de Guaranda para la autorización de romper calzada para la implementación del enlace son engorrosos.

Tomando en cuenta los estándares del cable UTP CAT 6 la máxima distancia permitida es de 200 metros. Un enlace con fibra óptica es muy costoso tanto por la fibra y sus elementos pasivos. Con estos antecedentes esta alternativa no es viable para dar solución a este problema.

Sabiendo, que la Casona Universitaria cuenta con una infraestructura para redes inalámbricas y tomando en cuenta la geografía del centro de la ciudad, la edificación y la vegetación, se ve la factibilidad de la implementación de un enlace por radio frecuencia desde la Casona Universitaria hacia la Casa Regional de Bolívar.

El costo de implementación es accesible ya que existen equipos de muy buena calidad disponibles en el mercado nacional y a precios cómodos, esta es la alternativa más viable para dar solución al problema.

Este enlace por radio frecuencia proporcionará el acceso a la red de datos y comunicación, que beneficiará las actividades investigativas, académicas y administrativas del Departamento y la Escuela que funcionan en La Casa Regional de Bolívar, además se integrará a la red de datos de La Universidad Estatal de Bolívar, permitiéndoles tener a su disposición las herramientas

tecnológicas necesarias para su mejor desenvolvimiento en sus labores cotidianas. De esta manera la Universidad ahorrará dinero y lo más importante tiempo.

Aprovechando la infraestructura del radio enlace, existirá la posibilidad de construir una red inalámbrica multipunto (Hot-Spots) que brindará el servicio de internet inalámbrico a la ciudadanía en especial a los docentes, trabajadores y estudiantes que se encuentren dentro del área de cobertura. Se ha realizado un censo rápido de los posibles usuarios de estos Hot-Spots los mismos que son: docentes y empleados de la Universidad Estatal de Bolívar y el rango de cobertura que se detallan a continuación:

NOMBRES	DIRECCIÓN	POTENCIA (dBm)	GANANCIA
ACURIO MILTON	7 DE MAYO Y OLMEDO	-69	EXCELENTE
AGUALONGO MYRIAN	7 DE MAYO Y SOLANDA	-87,5	BAJA
AGUILAR NERY	PICHINCHA 1008 Y GARCÍA MORENO	-87	BAJA
ALDAZ JAIME	CONVENCIÓN DE 1884 Y ROCAFUERTE	-88,5	BAJA
ARTEAGA TERESA	10 DE AGOSTO N903	-79	BUENA
CALLES JAIME	7 DE MAYO	-77	BUENA
CHIRIBOGA PATRICIO	AZUAY Y 7 DE MAYO	-89	BAJA
COLCHA ÁNGEL	PICHINCHA Y ESPEJO	-87,5	BAJA
DÁVILA LUIS	10 DE AGOSTO Y CORONEL GARCÍA	-79	BUENA
FERNÁNDEZ MARÍA	GARCÍA MORENO Y ANTIGUA COLOMBIA	-79	BUENA
FIERRO FABIÁN	ROCAFUERTE Y 9 DE ABRIL NO. 903	-87,5	BAJA
FIERRO WASHINGTON	ROCAFUERTE Y 9 DE ABRIL NO. 903	-87,5	BAJA
GONZÁLEZ LORENA	OLMEDO 114 Y SUCRE	-79	BUENA
GUEVARA EDELMIRA	CALLE 7 DE MAYO 411 Y 10 DE AGOSTO	-75	MUY BUENA
IBARRA JORGE	OLMEDO 514	-75	MUY BUENA
JARAMILLO RAMIRO	CONVENCIÓN Y 10 DE AGOSTO	-71,5	MUY BUENA
LARA PATRICIA	7 DE MAY0 y ROCAFUERTE	-88,5	BAJA
LEÓN MÓNICA	GARCÍA MORENO Y CORONEL GARCÍA	-88,5	BAJA
LUCIO AMARILIS	9 DE ABRIL Y ROCAFUERTE	-87,5	BAJA
NIETO HERNÁN	SUCRE 903 Y 10 DE AGOSTO	-81	BUENA
NOBOA DORIS	GARCÍA MORENO 903	-85	BUENA
PAREDES EDUARDO	7 DE MAYO N. 302 Y ROCAFUERTE	-86,5	BUENA

PROAÑO FLORA	PICHINCHA Y ESPEJO	-88,5	BAJA
ROSALES LUIS	10 DE AGOSTO 112 Y CORONEL GARCÍA	-80	BUENA
SALCEDO FRANCISCO	9 DE ABRIL Y ROCAFUERTE	-87,5	BAJA
SALTOS NELSON	SUCRE 801 Y OLMEDO	-83,5	BUENA
SÁNCHEZ MARÍA	CRNEL. GARCÍA 210 Y 10 DE AGOSTO	-84	BUENA
SECAIRA NELSON	CONVENCIÓN DE 1884 GARCÍA MORENO	-86	BUENA
TAMAYO RICHARD	CALLE ROCAFUERTE 916 Y 9 DE ABRIL	-88,5	BAJA
TORRES WILSON	9 DE ABRIL 405 Y OLMEDO	-82,5	BUENA
VALDIVIEZO FAUSTO	OLMEDO Y 9 DE ABRIL S/N	-87	BAJA
VALLEJO HENRY	CALLE 7 DE MAYO 411 Y 10 DE AGOSTO	-75	MUY BUENA
VERDEZOTO RAÚL	CALLE OLMEDO 705	-81,7	BUENA
ZAPATA ÁNGEL	ROCAFUERTE Y ANTIGUA COLOMBIA	-80,5	BUENA

Cuadro 2.1 Tabla de posibles usuarios de los Hot-Spots

Fuente: Creación propia

2.2. ESTUDIO DE FACTIBILIDAD

De acuerdo al análisis realizado, se determinó los requisitos mínimos de hardware y software.

2.2.1. Técnico y tecnológico

HARDWARE

Para determinar el hardware del enlace se realizo la comparación de tres marcas comerciales de equipos routers inalámbricos y se detallan a continuación:

MARCA	MODELO	CARACTERÍSTICAS	PRECIO ($)
LINKSYS	WRT54G	Router integral para uso compartido de internet, conmutador de 4 puertos y punto de acceso Wireless-G (802.11g) a 54 Mbps Permite compartir una conexión a Internet a otros recursos con dispositivos Ethernet con cables y Wireless-G y -B3 La función de configuración con sólo pulsar un botón hace que ésta sea simple y segura Alta seguridad: cifrado TKIP y AES, filtrado de direcciones MAC inalámbricas, potente firewall SPI	90.00

LINKSYS	WRT54GL V1.1	Permite la actualización del firmware tanto del fabricante como de terceros ya que incluye el sistema GNU/Linux, se puede actualizar con los firmware de Linksys para Linux o DD-WRT Puedes cambiar sus antenas y poner de mayor ganancia (7, 15 y hasta 24 dBi) Conexión de dispositivos 802.11b en 11Mbps y 802.11g en 54Mbps e inalámbricos a la red. Tipo de dispositivo Punto de Acceso, Router, Switch. Velocidades: 11 Mbps y 54 Mbps Seguridad: PSK, WEP - 128-bit, WEP - 64-bit, WPA, WPA2 Protocolo de transmisión de datos: IEEE 802,3, IEEE 802.CÚ, IEEE 802.11B, IEEE 802.11G	110.00
D-LINK	DI-524 WIRELES S ROUTER 11G, 54MBPS	Opera bajo los estándar Wi-Fi 802.11g. Hasta 54 Mbps de velocidad en la transmisión de datos. Firewall avanzado y control parental. Instalación simple y fácil. Estándar compatible con 802.11b. Fácil Instalación gracias al Soporte de UPnP	60.00
D-LINK	DI-624S SMB Wireless 108G USB Storage Router	Wireless storage router 108G. 4 puertos Ethernet 10/100Base-Tx. 2 puertos USB 2.0 para conexión de impresora/disco duro. Control parental. Servidor de archivos para compartir datos/espacio. Servidor FTP para compartir archivos	168.00
3COM	3012	Routers de acceso WAN económicos y ricos en funcionalidad con firewall y funciones de seguridad para VPNs y una gran variedad de interfaces, para oficinas remotas.	725.00
3COM	6080	Con amplia variedad de características, tolerantes a fallos y de alto rendimiento, que proporcionan convergencia de voz y datos de extremo a extremo. Routing de alto rendimiento con características avanzadas de administración de tráfico, seguridad y control. Una gama de Tarjetas de Interfaz Flexible (FICs) para LAN y WAN intercambiables en caliente proporciona un funcionamiento de la red escalable, eficiente y seguro.	546.00

Cuadro. 2.2 Marcas de equipos inalámbricos del mercado nacional

Fuente: Creación propia

Una vez realizado el análisis de cada uno de los equipos: 3COM, D-Link y Linksys. Se llegó a determinar que el equipo router inalámbrico apropiado para el enlace por radio frecuencia entre la Casona Universitaria y la Casa Regional de Bolívar, es el router marca Linksys modelo WRT54GL v1.1, el cual permite la manipulación de su hardware (extracción de la tarjeta electrónica) y su software (actualización del firmware Linux Thibor). Estos equipos se los puede encontrar en el mercado nacional y lo más importante a precios accesibles

Es router inalámbrico tiene compatibilidad con los estándares wireless 802.11b en 11Mbps y 802.11g en 54Mbps, También se configura como Access Point y permite dar seguridades a través de los distintos cifrados.

Cabe mencionar que no se tomó en cuenta los router inalámbricos marca Cisco, por las características del enlace y por los precios que son muy elevados.

GPS.- (Global Positioning System) Sistema de Posicionamiento Global es un sistema de posicionamiento terrestre, la posición la calculan los receptores GPS gracias a la información recibida desde satélites en órbita alrededor de la Tierra.

El patrón de medición del GPS son las unidades UTM las cuales se transforman a unidades geográficas: altitud, latitud y longitud.

Con el GPS se obtuvieron las coordenadas reales de los tres puntos de instalación, lo que permitió el diseño real de la trayectoria del enlace entre la Casona Universitaria y la Casa Regional de Bolívar.

Antenas Direccionales.- Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance, entre estas tenemos:

> **Antenas Bi-Quad.-** Pertenece al grupo de las antenas sectoriales y directivas, es decir, concentra su efectividad en un sentido y dirección principalmente, la ganancia de esta antena es en el orden de 11 a 12 dBi, trabaja en la frecuencia de 2.4 Ghz y su alcance es aproximadamente 1km.

Doble Bi-Quad.- Es igual a la antena anterior pero a esta le son adicionados dos cuadros más. El resultado de esta modificación es un aumento en la ganancia de la antena del orden de 24 dBi, de igual forma trabaja en la frecuencia 2.4 Ghz y su alcance es aproximadamente de 2km.

Antenas Omnidireccionales.- Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Existen antenas omnidireccionales de 8, 12, 16 dBi.

Antenas Sectoriales.- Emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional, el alcance de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

Una vez hecho el análisis de las antenas se concluyó que la antena más adecuada para el enlace por radio es la antena direccional de Bi-Quad, tomando en cuenta que la distancia máxima a cubrir es de 300 m. y utiliza la misma frecuencia del router (2.4 Ghz).

Para la red inalámbrica multipunto (Hot-Spots) se concluyó que la antena omnidireccional más adecuada fue la de 8 dBi, con un alcance de 200 m.

La construcción de las antenas direccionales de Bi-Quad y omnidireccionales, se realizó con elementos, materiales y herramientas que se encontraron en el mercado local y nacional a bajos precios.

SOFTWARE (FIRMWARE)

Para determinar el software del router inalámbrico se realizó la comparación de los firmwares que se detallan a continuación:

FIRMWARE	DESCRIPCIÓN
Hyperwrt _G_ Thibor 15c	El kernel es Linux La potencia del equipo se lo puede aumentar de forma manual lo que nos permite adaptar antenas de mayor ganancia. Tiene incluido el Demonio Kai para el Kai Console Gaming network, WDS Puente de red/repetidor, Autenticación Radius lo cual permite comunicaciones Wireless más seguras, y Calidad de servicio (QOS).
DD-WRT	Es un firmware no-oficial para Linksys WRT54G/GS/GL y otros routers 802.11g basados en un diseño de referencia similar o igual al Broadcom. Es un firmware Beta, por ello contiene errores. No es recomendable instalar firmwares beta en redes grandes. El firmware oficial de linksys no incluye, DD-WRT añade el Demonio Kai para el Kai Console Gaming network, WDS Puente de red/repetidor, Autenticación Radius para comunicaciones Wireless más seguras, avanzado control de balanceo de cargas o Calidad de servicio (QOS), y software para que funcionen las tarjetas SD/MMC que se le pueden instalar haciendo algunas modificaciones al dispositivo. Ocupa demasiada memoria del equipo

Cuadro.2.3 Comparación de Firmwares

Fuente: Creación propia

Una vez realizado el análisis de los firmwares se llegó a la conclusión que el Firmware Hyperwrt _G_ Thibor 15c, fue el adecuado para el enlace por radio frecuencia por sus características. Además esté se acopló de manera excelente al router inalámbrico seleccionado, las interfaces del nuevo firmware son amigables al usuario, cabe recalcar que una característica importante de esté es permitir el aumento de la potencia del radio y cambiar las antenas por unas de mayor ganancia por ejemplo: 8, 12, 16 hasta 24dBi.

El Software de Diseño Radio Mobile.- De la empresa 'Agilent' Con el fin de simular y predecir el comportamiento de la red, y así hacer un diseño más realista se utilizó el software Radio Mobile. Este software permite calcular radioenlaces para cualquier tipo de tecnología, se puede escoger la frecuencia a la que se quiere trabajar, los tipos de antena, la potencia transmitida y muchos otros parámetros.

Trabajar con coordenadas reales, de manera que se pueden utilizar mapas de la región que se necesite. Estos mapas incluyen información cartográfica del terreno, permiten saber la altura de cada punto, así como la presencia de ríos, montañas y demás accidentes geográficos, un área curvas de nivel. Previamente al diseño final se realizó una visita a la zona, para tomar coordenadas con un GPS, para comprobar las condiciones generales, valorar las alturas de los obstáculos, etc. Con esta información se procedió al cálculo de los radioenlaces con este software.

Ping.- Este software ayuda a determinar dónde se encuentra exactamente un problema de la conexión. Utiliza paquetes ICMP para intentar contactar un servidor específico e informa cuánto tiempo lleva obtener una respuesta.

Para terminar de colectar datos se presiona control-C. Si los paquetes se toman mucho tiempo en regresar puede haber una congestión en la red. Si el retorno de los paquetes de contacto tiene un TTL inusualmente bajo, puede que haya problemas de enrutamiento entre la computadora y el extremo remoto.

Iperf.- Es un software de línea de comandos y ahora de modo grafico para estimar el rendimiento de una conexión de red. Utiliza un modelo "cliente" y "servidor". Para correr iperf, se inicia un servidor en un lado y un cliente en el otro:

El lado del servidor continuará escuchando y aceptando conexiones del cliente en el puerto 5001 hasta que se presione control-C para detenerlo, incluye soporte IPv6.

Esta herramienta ayuda a ver cuán rápido puede funcionar el enlace, cuál es su capacidad real utilizable, es decir poder obtener una estimación de la capacidad de rendimiento con tráfico y sin tráfico y midiendo cuánto demora en transferir los datos.

Netstumbler.- Este software para detectar redes inalámbricas (monitoreo) utilizando Microsoft Windows. Soporta una variedad de tarjetas inalámbricas. Detecta redes abiertas y encriptadas, pero no puede detectar redes inalámbricas "cerradas". También ofrece un medidor de señal/ruido que grafica la señal recibida a lo largo del tiempo. También se puede integrar con una variedad de dispositivos GPS, para registrar ubicaciones precisas e información sobre la potencia de la señal. Todo esto hace que Netstumbler sea una herramienta accesible para realizar una prospección informal de la zona.

Esta herramienta de monitoreo, nos provee una lista de redes inalámbricas disponibles con información básica tales como: intensidad de la señal y canal SSDI, encript. Lo que nos permite detectar rápidamente redes cercanas y determinar si están dentro de nuestro alcance o si están causando interferencia.

RxTx.- Mide el ancho de banda de transferencia de datos entre la computadora y servidores múltiples. Trabaja DIALUP cable, o las conexiones de DSL. El ancho de banda es medido descargando uno o más archivos de HTTP y estimar el promedio de datos recibidos.

Además, RxTx exhibe velocidades de datos instantáneos y medios en tiempo real. Las velocidades de datos son indicados en kbps (kilo bits por segundos) o KBs/s (kilo bytes por segundo).

2.2.2. Recursos Humanos

Este proyecto de grado se lo realizó con la intervención de las siguientes personas:

Asesor de tesis: Dr. Henry Vallejo Ballesteros, quien se encargó del asesoramiento de las actividades realizadas durante el desarrollo del proyecto de grado.

Colaborador: Ing. Juan Gaibor, quien impartió sus conocimiento en relación a los aspectos metodológicos para un buen desarrollo del proyecto de graduación.

2.2.3. Económico Financiero

Tomando en cuenta la trayectoria del enlace por radio frecuencia entre La Casona Universitaria y La Casa Regional de Bolívar, para su implementación se adquirió: equipos routers inalámbricos Linksys, elementos para la construcción de antenas direccionales y omnidireccionales, así como también materiales necesarios para su implantación.

Los costos de los equipos, elementos y materiales para la implementación se detallan a continuación:

Descripción	**Unidad**	**Cantidad**	**Precio Unitario($)**	**Total($)**
Router Linksys WRT 54GL V1.1	Unidad	6	110,00	660,00
Switch C-Net	Unidad	1	18,00	18,00
GPS Magellan Triton	Unidad	1	0,00	0,00
Computadora portátil	Unidad	1	680,00	680,00
Cámara Digital	Unidad	1	280,00	280,00
Pigtail	Unidad	9	25,00	225,00
Jack N chasis cuadrado hembra	Unidad	10	5,00	50,00
Cable eléctrico	Metro	100	0,30	30,00
Cable UTP CAT 5	Metro	100	0,35	35,00
Caja hermética 30x20x15cm.	Unidad	3	18,60	55,80
Caja plástica	Unidad	6	0,80	4,80
Alambre galvanizado	Libra	4	1.10	4.40
Tubo de aluminio de 1 3/4 pulgadas	Unidad	1	20,94	20,94

Tubo eléctrico PVC	Unidad	1	1,00	1,00
Manguera espiral	Metro	100	0,35	35,00
Tubo de cañería de ½ de diámetro	Metro	1	5,00	5,00
Tubo de cañería de ¼ de diámetro	Metro	3	3,00	9,00
Alambre de cobre # 16	Metro	10	0,28	2,80
Cerrajería Brazos y bases metálicos	Unidad	9	3,70	33,30
Baquelita	Unidad	5	2,0	10,00
Conectores RJ45	Unidad	30	0,10	3,00
Botas para conectores RJ45	Unidad	30	0,03	0,90
Abrazadera galvanizada	Unidad	8	0,15	1,20
Espesor de viento	Libras	10	0,70	7,00
Tensado de los vientos	Unidad	6	0,70	4,20
Cáncamos	Unidad	6	0,50	3,00
Taco fisher	Unidad	20	0,02	0,40
Tornillo para gabinetes metálicos	Unidad	6	0,50	3,00
Tornillo con mariposa	Unidad	5	0,30	1,50
Tornillos para sujetar router y bovinas	Unidad	12	0,10	1,20
Estaño y crema para soldar	Unidad	1	60,00	60,00
Tomas Corriente	Unidad	5	0,60	3,00
Enchufe	Unidad	3	0,25	0,75
Autofundente	Rollo	2	7,20	14,40
Taipe	Unidad	3	0,35	1,05
Adhesivo líquido	Unidad	1	1,50	1,50
Silicona en barra	Unidad	20	0,20	4,00
Silicona líquida	Unidad	2	2,80	5,60
Epóxica	Unidad	1	3,00	3,00
Masilla epóxica	Unidad	2	2,00	4,00
Laca transparente	Unidad	1	2,10	2,10
Pintura anticorrosivo plateado	Unidad	1	2,10	2,10
Amarras grandes	Funda	1	3,00	3,00
Amarras pequeñas	Funda	1	2,50	2,50
Lija de agua	Unidad	1	0,40	0,40
Pistola para silicona	Unidad	1	6,00	6,00
Pistola para epóxica	Unidad	1	1,50	1,50
Lima de acero	Unidad	1	3,20	3,20
Sierra de arca	Unidad	1	6,00	6,00
Sierra	Unidad	1	1,20	1,20

Broca para taco Fisher 12	Unidad	1	0,50	0,50
Broca para taco Fisher 10	Funda	1	0,50	0,50
Regla milimetrada	Unidad	1	15,00	15,00
Kit de red (ponchadora RJ45, cortadora, tijera, lantester).	Unidad	1	80,00	80,00
Kit de herramientas (destornilladores, llaves metálicas, hexagonales)	Unidad	1	80,0	80,00
Binoculares	Unidad	1	20,00	20,00
Cautín	Unidad	1	12,00	12,00
Varios			50,00	50,00
TOTAL				**2569,74**

Cuadro.2.4 Presupuesto del proyecto

Fuente: Creación propia

El costo de la implementación del enlace por radio frecuencia entre la Casona Universitaria y la Casa Regional de Bolívar fue de USD **2569,74** dólares americanos, monto que asumieron las estudiantes proponentes del proyecto de grado, como una contribución al proyecto de Redes Inalámbricas de la Universidad Estatal de Bolívar y al desarrollo de las redes de datos del campus Universitario.

El enlace por radio con otros equipos inalámbricos y a cargo de una empresa le costaría a la Universidad una inversión aproximada de $ 4.200,00, por lo que este trabajo de investigación determinó un ahorro a la Universidad de $ 1.630,00 dólares americanos.

2.3. DISEÑO DE LA TRAYECTORIA DEL ENLACE POR RADIO

Para la realización del diseño de la trayectoria del enlace entre la Casona Universitaria y la Casa Regional de Bolívar se tomo en cuenta los siguientes aspectos.

Línea de Vista.- Si podemos ver un punto A desde un punto B tenemos línea visual. La línea visual que necesitamos para tener una conexión inalámbrica óptima desde A hasta B es una elipse. Su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

Zona de Fresnel.- La teoría de zona de Fresnel simplemente examina a la línea desde A hasta B y luego el espacio alrededor de esa línea que contribuye a lo que está llegando al punto B. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas. Consecuentemente, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos.

Existen muchas zonas de Fresnel, pero principalmente la zona 1 es la más importante. Si esta fuera bloqueada por un obstáculo, como un árbol o un edificio, la señal que llegue al destino lejano será atenuada. En enlaces inalámbricos, se debe asegurar de que esta zona va a estar libre de obstáculos, por lo menos el 60% de la primera zona de Fresnel.

Utilizando la técnica de observación directa, se llegó a determinar que no hay punto de vista directa porque la segunda torre de la Catedral "San Pedro de Guaranda" interfiere la visibilidad entre la Casona Universitaria y la Casa Regional de Bolívar como se muestra en la figura 2.1, lo cual estableció la necesidad de implementar un punto intermedio en la trayectoria del enlace.

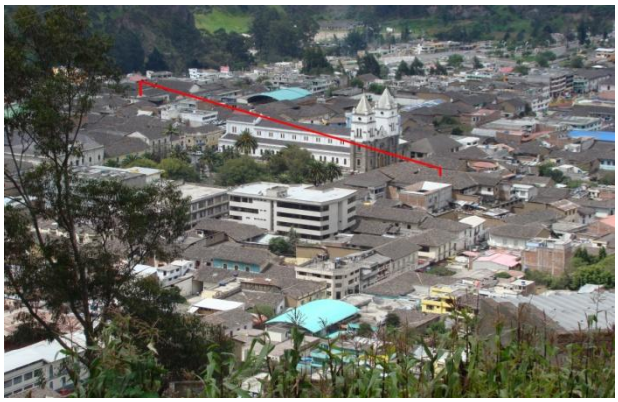


Fig. 2.1 Observación directa entre la Casona Universitaria-Casa Regional de Bolívar

Fuente: Creación propia

Una vez analizados estos aspectos y con la observación directa se determinó la trayectoria del enlace. Se hizo referencia a un punto intermedio el mismo que tenía línea visual directa tanto a la Casona Universitaria y la Casa Regional de Bolívar; este punto intermedio no debe tener ninguna interferencia de árboles ni edificaciones.

Desde la torre de la Casona Universitaria se observó el edificio de la Curia como la edificación más alta, para comprobar subimos a la cornisa de la Casa Regional de Bolívar y efectivamente el edificio de la Curia "Obispado" es el punto estratégico para el repetidor como se puede observar a continuación.

Fig. 2.2 Trayectoria del enlace

Fuente: Creación propia

Se solicitó autorización para ir a la azotea del edificio, confirmando que éste es el punto adecuado para el repetidor, la azotea es de concreto donde se instaló el mástil.

Se utilizó el software de diseño Radio Mobile y GPS para determinar la trayectoria del enlace técnicamente. Las coordenadas obtenidas a través del GPS en los tres puntos:

La Casona Universitaria Zona 17S

UTM

X: 17S722264E

Y: 9823884N

Latitud: -1.592398057247037

Longitud: -79.0022100609756

Altura: 2705 m

Obispado Zona 17S

UTM

X: 17S722437E

Y: 9823887N

Latitud: -1.592369415292198

Longitud: -79.0006557356373

Altura: 2709 m

La Casa Regional de Bolívar Zona 17S

UTM

X: 17S722486E

Y: 9823809N

Latitud: -1.5930742377641773

Longitud: -79.00021480592788

Altura: 2706 m

MAPA CURVAS DE NIVEL DE LA PROVINCIA BOLÍVAR

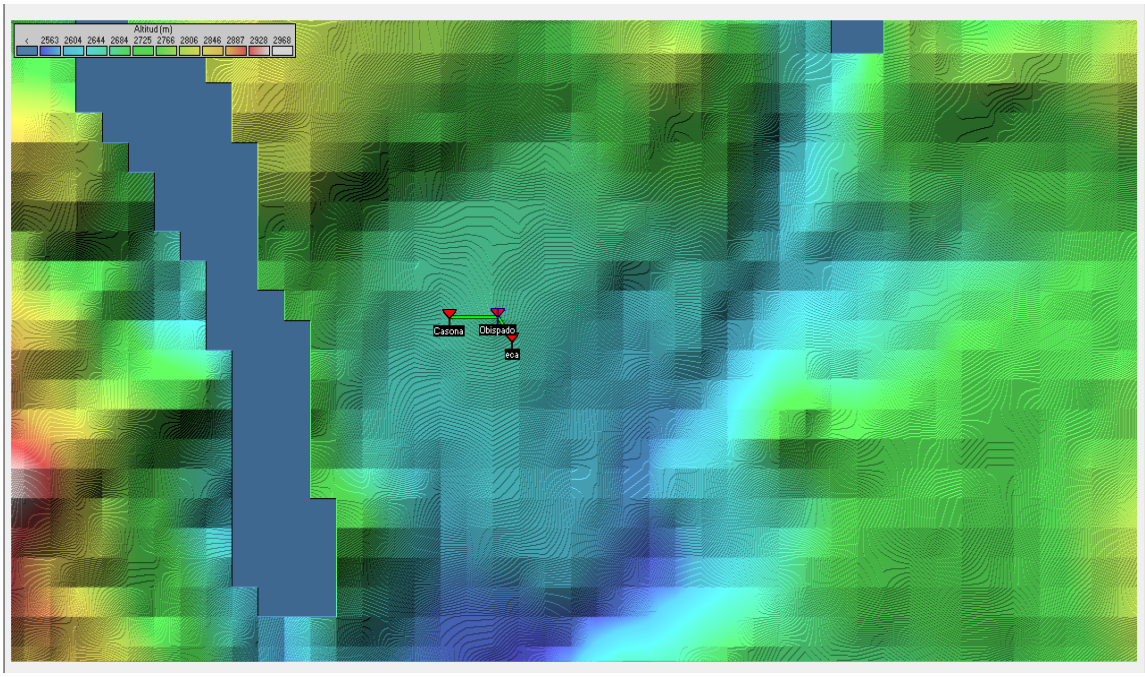


Fig. 2.3 Curvas de nivel de la provincia Bolívar

Fuente: IGM Instituto Geográfico Militar – 2009

Para la realización del diseño gráfico del enlace se utilizó el mapa de las curvas de nivel de la ciudad de Guaranda, en el cuál se gráfica los puntos de la trayectoria del enlace para determinar la factibilidad del proyecto.

CURVAS DE NIVEL

Fig. 2.4 Trayectoria del enlace

Fuente: IGM Instituto Geográfico Militar - 2009

DISEÑO DEL ENLACE CASONA UNIVERSITARIA-OBISPADO

Los datos obtenidos del GPS fueron ingresados al Software Radio Mobile para la realización de los cálculos respectivos que determinaron la factibilidad técnica del enlace, y se observo el área de la zona de Fresnel como se muestra en la figura.

CASONA UNIVERSITARIA-OBISPADO

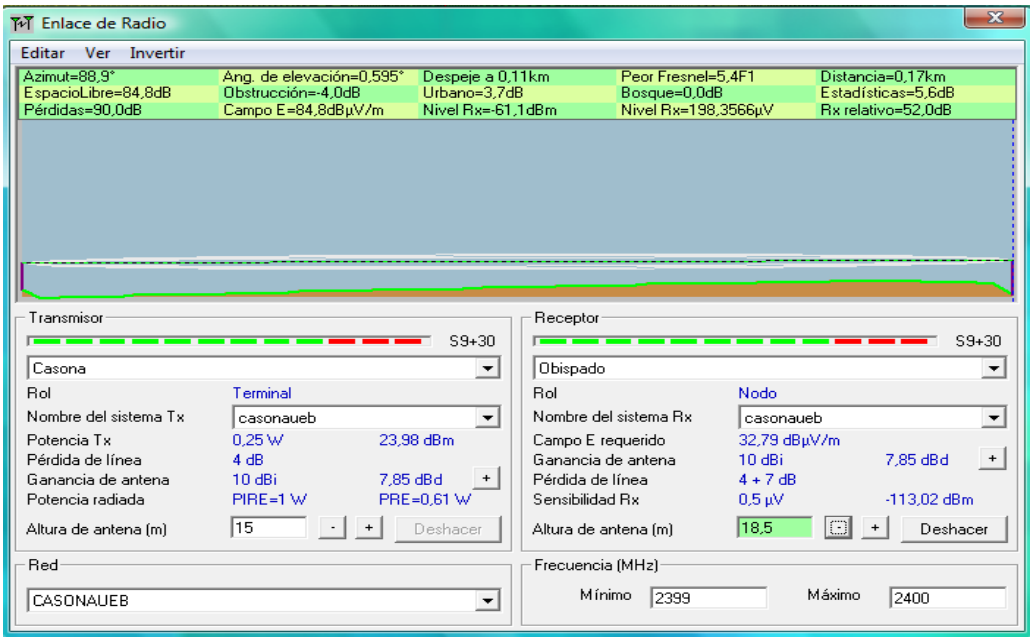


Fig. 2.5 Zona de Fresnel Casona – Obispado

Fuente: Creación propia

Análisis de los resultados

La distancia entre La Casona y Obispado es 0,2 Km (0,1 millas)

Azimut norte verdadero = 88,9°, Azimut Norte Magnético = 90,4°, Angulo de elevación = 0,5946°

Variación de altitud de 10,0 m

El modo de propagación es mediante uso de línea de vista, mínimo despeje 5,4F1 a 0,1km

La frecuencia promedio es 2399,500 MHz

Espacio Libre = 84,8 dB, Obstrucción = -4,0 dB, Urbano = 3,7 dB, Bosque = 0,0 dB, Estadísticas = 5,6 dB

La Ganancia del sistema de Casona a Obispado es de 142,0 dB (antena Bi-Quad a 88,9° ganancia = 10,0 dBi)

La Ganancia del sistema de Obispado a Casona es de 142,0 dB (antena Bi-Quad a 268,9° ganancia = 10,0 dBi)

La peor recepción es 52,0 dB sobre la señal requerida a encontrar, esto se refiere a los pequeños lóbulos que irradian en la parte posterior del biquad donde la transmisión es nula.

El umbral de recepción (limite del enlace) entre La Casona Universitaria y Obispado se puede observar en la siguiente gráfica.

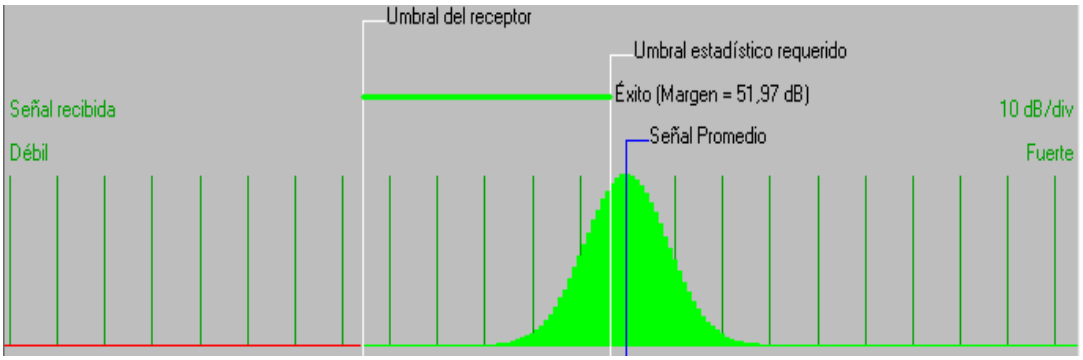


Fig. 2.6 Umbral de recepción Casona Universitaria – Obispado

Fuente: Creación propia

DISEÑO DEL ENLACE OBISPADO - CASA REGIONAL DE BOLÍVAR

Se realizó el mismo procedimiento y se observar la zona de Fresnel como se muestra en la figura.

OBISPADO – CASA REGIONAL DE BOLÍVAR

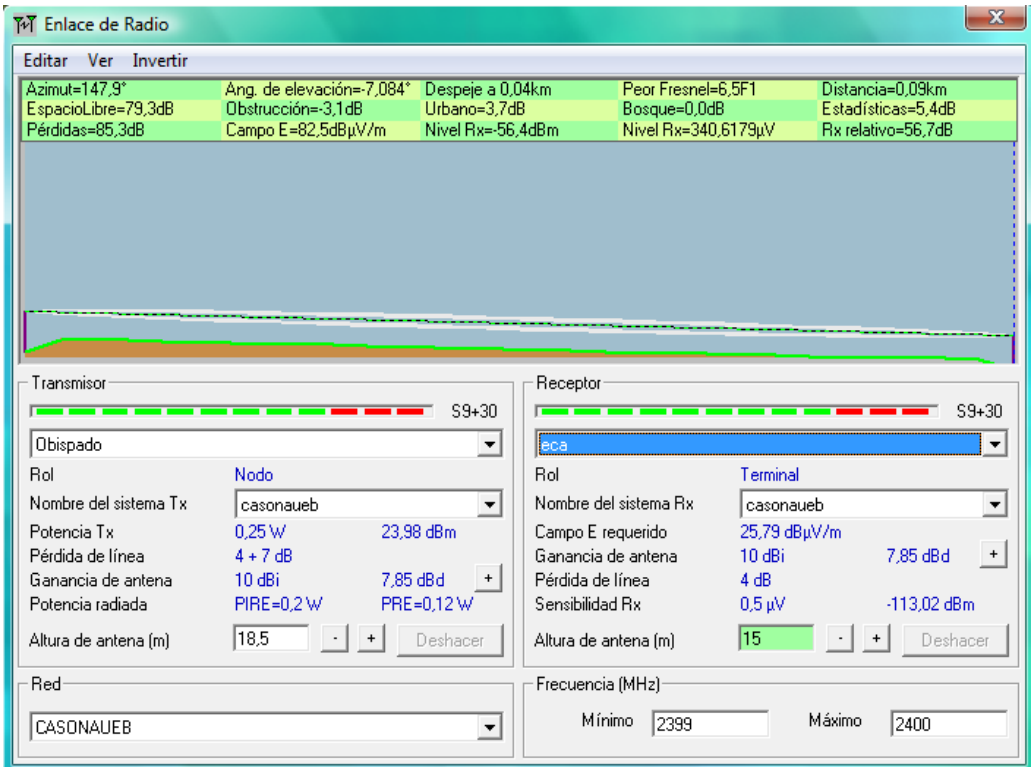


Fig. 2.7 Zona de Fresnel Obispado- Casa Regional De Bolívar

Fuente: Creación propia

Análisis de los resultados:

La distancia entre Obispado y La Casa regional de Bolívar es 0,1 km (0,1 millas)

Azimut norte verdadero = 147,9°, Azimut Norte Magnético = 149,4°, Angulo de elevación = -7,0838°

Variación de altitud de 9,0 m

El modo de propagación es mediante uso de línea de vista, mínimo despeje 6,5F1 a 0,0km

La frecuencia promedio es 2399,500 MHz

Espacio Libre = 79,3 dB, Obstrucción = -3,1 dB, Urbano = 3,7 dB, Bosque = 0,0 dB, Estadísticas = 5,4 dB

La pérdida de propagación total es 85,3 dB

La Ganancia del sistema de Obispado a Ecca es de 142,0 dB (antena Bi-Quad a 147,9° ganancia = 10,0 dBi)

La Ganancia del sistema de Ecca a Obispado es de 142,0 dB (antena Bi-Quad a 327,9° ganancia = 10,0 dBi)

La peor recepción es 56,7 dB sobre la señal requerida a encontrar, esto se refiere a los pequeños lóbulos que irradian en la parte posterior del bi-quad donde la transmisión es nula.

El umbral de recepción entre el Obispado y La Casa Regional de Bolívar es el que se muestra en la gráfica

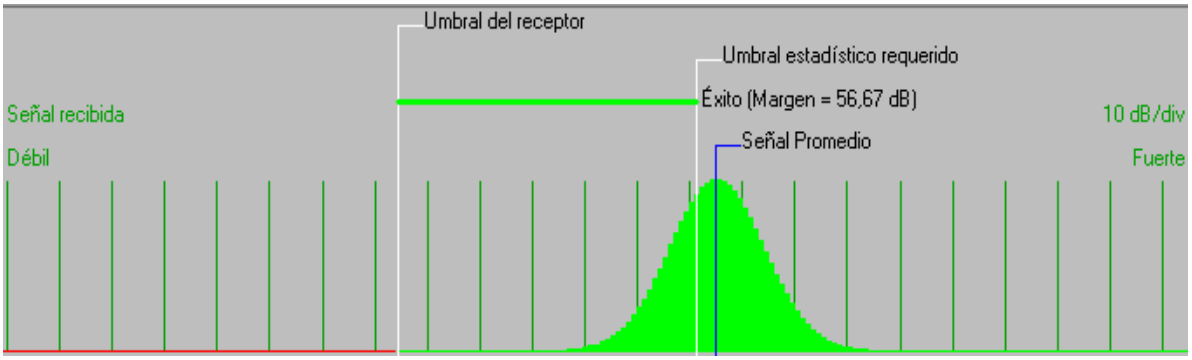


Fig. 2.8 Umbral de recepción Obispado – Casa Regional de Bolívar

Fuente: Creación propia

Por medio de este software se concluyó que el enlace por radio entre la Casona Universitaria y la Casa Regional de Bolívar es factible técnicamente.

Inmediatamente se construyó dos antenas directivas Bi-Quad de 12bdi. Para ello se requirió los siguientes materiales: placa de baquelita, cable de cobre de 16mm, conector Jack N chasis, cautín, estaño, crema de soldar, taladro, broca #12, sierra, regla milimetrada, lima de acero, pinzas.

Ganancia de las antenas

Antenas direccionales

Eficiencia de la antena (nt)	*Donde:*
$nt = \frac{Rt}{Rt + Rp}$	Rt=Resistencia de Radiación(energía - irradia al espacio)= 100Mw Rp=Resistencia de pérdidas (conector y pigtail) 0.25+0.5= 0.75
Densidad de potencia de la antena (s)	
$s = \frac{Pt}{4\pi d^2}$ [W/m²]	Pt = Potencia Transmitida (Radio) = 100mW (0.1W) d= Distancia entre antenas (Casona-Obispado) = 200m y 100m (Obispado - Casa Regional de Bolivar)
Directividad (D)	
$D = \frac{S}{Siso}$	S =Densidad de potencia de la antena $Siso$ =Densidad de potencia de la antena isotrópica
Ganancia de las antennas directivas (G)	
$G = nt * D$	nt= eficiencia de las antennas D = Directividad

$nt = \frac{100}{100+0.75} = \frac{100}{100.75} = 0.99 = 1\%$

$Siso = \frac{0.1}{4.\pi.(1*1)} = 0.00796$ Densidad isotrópico

$S = \frac{0.1}{4.\pi.(200*200)} = 1.98 \text{ x } 10^{-7}$ Casona - Obispado

$S = \frac{0.1}{4.\pi.(100*100)} = 7.96 \text{ x } 10^{-7}$ Obispado-Casa Regional de Bolivar

$D = \frac{1.98 \text{ x } 10 -7}{0.00796} = 2.49 \text{ x} 10^{-5}$ Casona – Obispado

$D = \frac{7.96 \text{ x } 10 -7}{0.00796} = 1 \text{ x} 10^{-4}$ Obispado - Casa Regional de Bolivar

$G=1*2.49 \text{ x} 10^{-5}= 2.49 \text{ x} 10^{-5}$ Casona-Obispado

$G=1*1 \text{ x} 10^{-4}= 1 \text{ x} 10^{-4}$ Obispado-Casa Regional de Bolivar

Antena Omnidireccional

$S = \frac{0.1}{4.\pi.(300*300)} = 8.84 \text{ x } 10^{-8}$ Densidad de omnidireccional

$D = \frac{8.84 \text{ x } 10 -8}{0.00796} = 1.11 \text{x} 10^{-5}$ Directividad

$G=1*1.11 \text{ x} 10^{-5}= 1.11 \text{ x} 10^{-5}$ Ganancia de la antena omnidireccional

2.3.1 Pasos para la Construcción de la Antena Direccional Bi-Quad

1. Se cortó la baquelita en forma de cuadrado, de la siguiente dimensión 12,3 cm x 12,3 cm utilizando la regla milimetrada, sierra y la sierra de arco.

Fig. 2.9 Medir la baquelita
Fuente: Creación propia

Fig. 2.10 Cortar la baquelita
Fuente: Creación propia

2. Se marcó en la parte central de la placa de baquelita un punto de referencia y se hizo un agujero con la broca #12 utilizando el taladro; se procedió a limar el agujero para eliminar limallas.

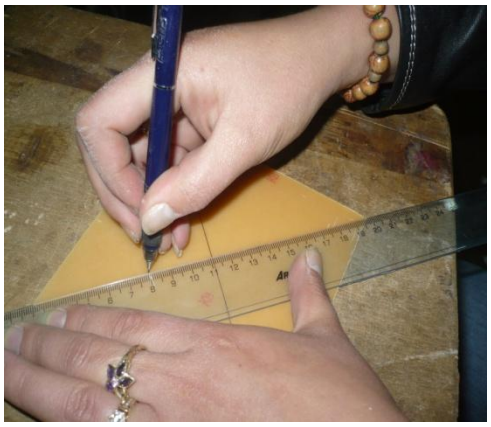


Fig. 2.11 Marcar el punto de referencia
Fuente: Creación propia

Fig. 2.12 Hacer el agujero en la baquelita
Fuente: Creación propia

3. Se colocó el conector Jack N chasis en el agujero y con los remaches top se sujetó a la placa con la pistola remachadora.

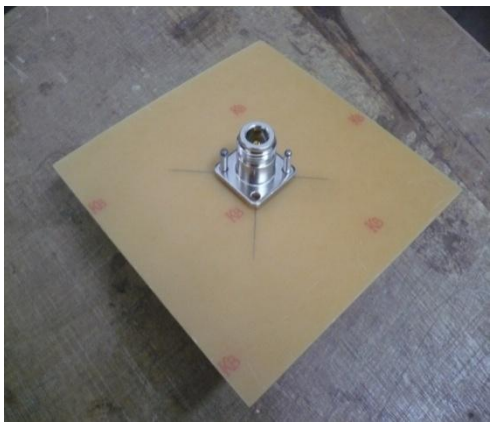


Fig. 2.13 Colocar los remachar
Fuente: Creación propia

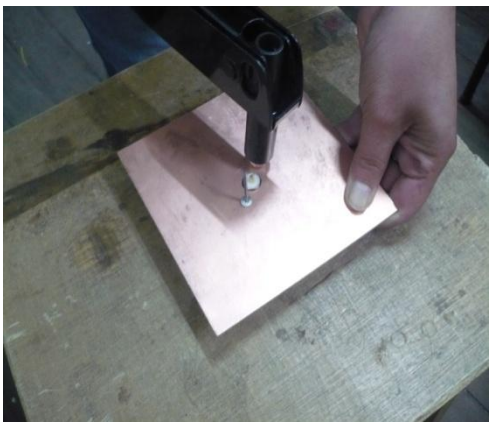


Fig.2.14 Remachar el conector
Fuente: Creación propia

4. En las siguientes graficas se observa el conector sujeto a la parte superior y posterior de la placa

Fig. 2.15 Placa parte superior
Fuente: Creación propia

Fig. 2.16 Placa parte posterior
Fuente: Creación propia

Pasos para la construcción del Bi-Quad.

5. Se midió con la regla milimetrada un segmento de 26,4 cm de cable de cobre #16, luego se procedió a corta con el cortafuego y se retiró el aislante

a. Se midió el punto central del cable 13.2 cm y con la pinza se hizo un doblez de 90º formando una V.

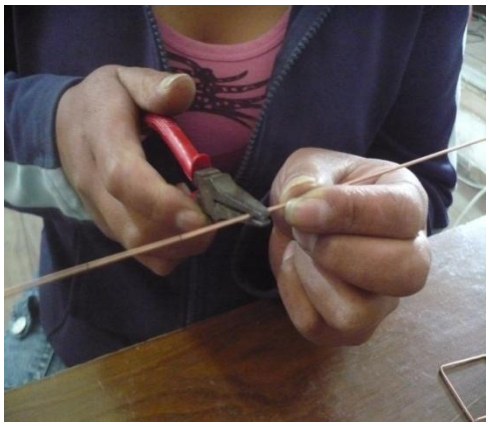


Fig. 2.17 Doblez de 90º al cable de cobre
Fuente: Creación propia

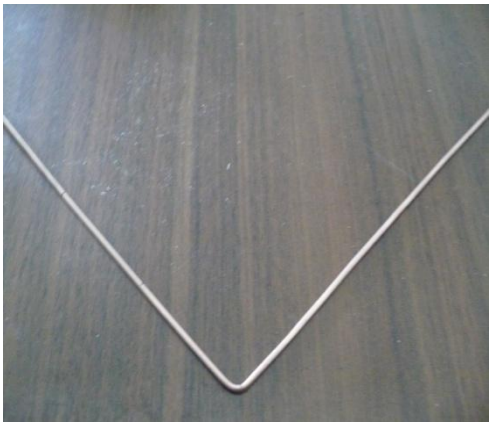


Fig. 2.18 Cable de cobre en forma de V
Fuente: Creación propia

b. Se cogió un lado de 13.2 cm este se dividió para 4, cada lado tiene 3.3 cm para formar un cuadrado del Bi-Quad, en el primer punto medido con la pinza se hizo un doblez de 90º y se repitió este proceso en el otro lado formando una M.

Fig. 2.19 Hacer un doblez de 90º
Fuente: Creación propia

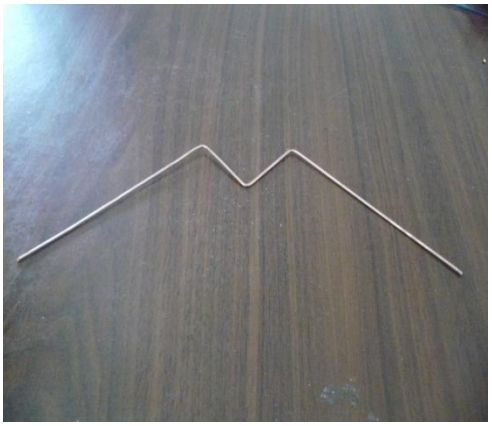


Fig. 2.20 Cable de cobre en forma de M
Fuente: Creación propia

c. En el segundo punto medido con la pinza se realizó nuevamente un doblez de 90º y de igual forma en el otro lado.

Fig. 2.21 Doblez de 90º al cable
Fuente: Creación propia

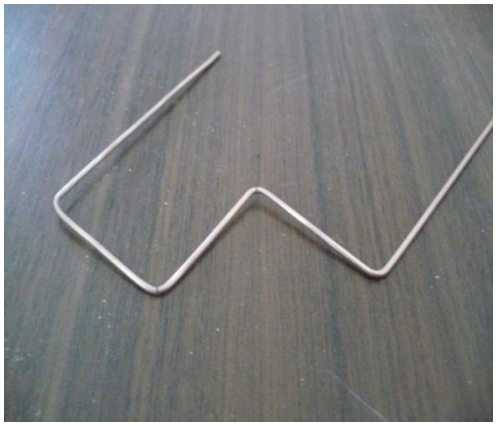


Fig. 2.22 Formar el cuadrado de Bi-Quad
Fuente: Creación propia

d. Se Realizó el último doblez de 90º con la pinza, formando los cuadrados del Bi-Quad como se observa en la figura.

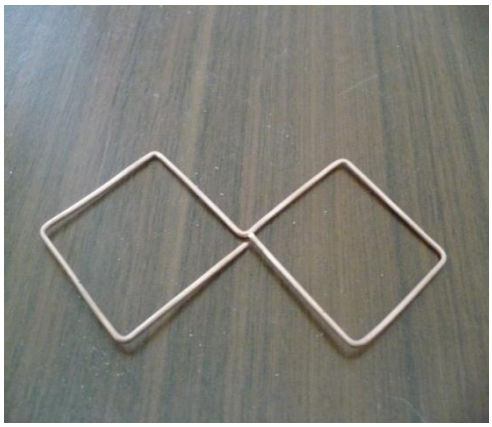


Fig. 2.23 Bi-Quad terminado
Fuente: Creación propia

Terminada la construcción del Bi-Quad se continuó la construcción de la antena.

6. Se cortó el cable de cobre en dos segmentos de 1,5 cm de longitud, se procedió a soldar el primer segmento en el pin del Jack N chasis y el otro extremo se soldó en el centro del Biquad; el segundo segmento soldado en el negativo del conector

y el otro se soldó con los extremos del Biquad, para este paso se utilizó un cautín, estaño, crema de soldar y una pinza.

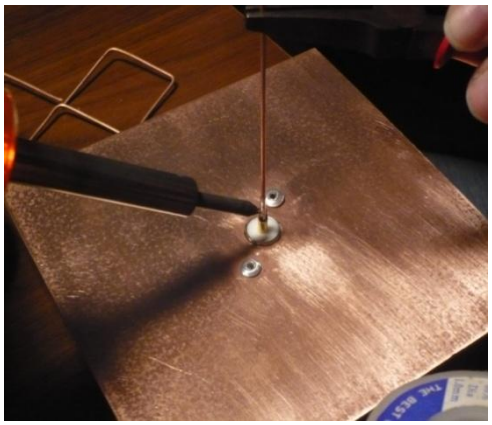


Fig. 2.24 Soldar en el pin del Jack N
Fuente: Creación propia

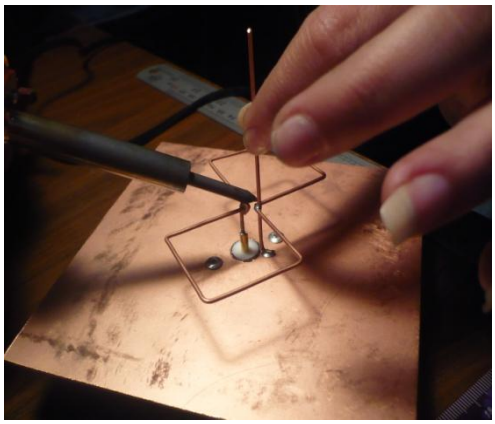


Fig. 2.25 Soldar los extremos del biquad
Fuente: Creación propia

Se trató que la suelda no se derrame sobre la placa, otro aspecto que se tomó en cuenta es no hacer grumos de suelda.

7. Se lijó la placa de baquelita para eliminar cualquier impureza.

Fig. 2.26 Ligado de la placa de baquelita
Fuente: Creación propia

8. Se realizó el lacado de la placa de la baquelita para evitar la oxidación del bronce.

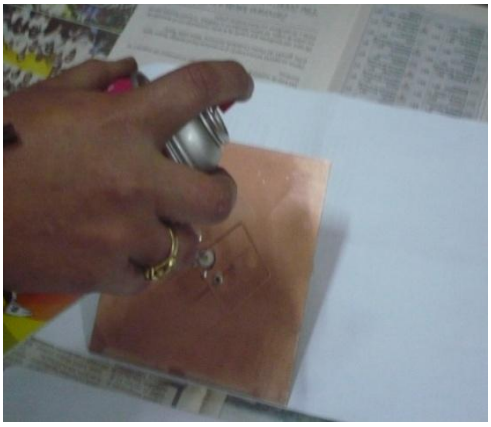


Fig. 2.27 Lacado de la placa de la baquelita

Fuente: Creación propia.

9. Antena de Bi-Quad terminada.

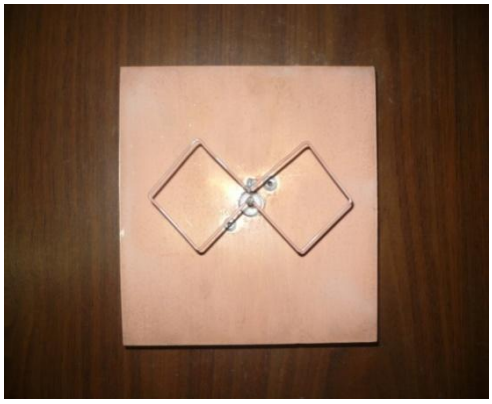


Fig. 2.28 Antena de Bi-Quad

Fuente: Creación propia.

Para probar la ganancia de la antena se requirió de un equipo activo el router inalámbrico Linksys WRT54GL v1.1.

2.3.2 Pasos para la repotencialización del equipo Linksys.

1. Se conectó la corriente eléctrica al router y el cable de datos, un extremo de cable de datos al primer puerto de la LAN y el otro a la computadora portátil.

2. Se ingresó al menú de configuración del router, a través del browser utilizando un navegador Web que pueden ser: Mozilla, Internet Explorer, etc.

   Se escribió en la URL la dirección que viene por defecto en el router *192.168.1.1*. Se desplegó la ventana de identificación requerida.

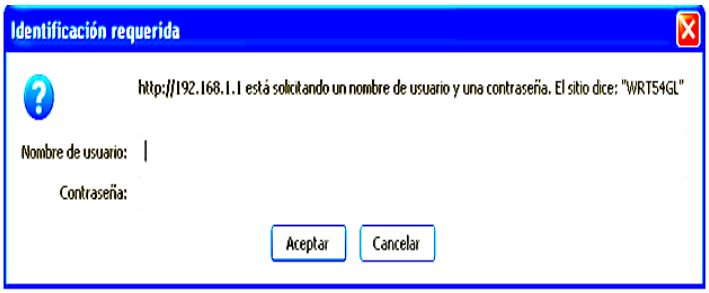


Fig. 2.29 Identificación requerida

Fuente: Creación propia.

3. Se ingresó el nombre de usuario "*root*" y la contraseña "*admin*", que vienen por defecto, por seguridad se recomienda cambiar el nombre de usuario y contraseña.

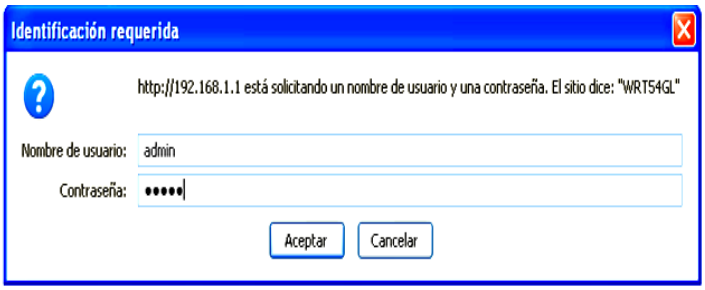


Fig. 2.30 Ingrese el nombre de usuario y la contraseña

Fuente: Creación propia.

4. Se desplegó la pantalla principal del software del equipo firmware versión: v4.30.11, se observó la configuración del setup.

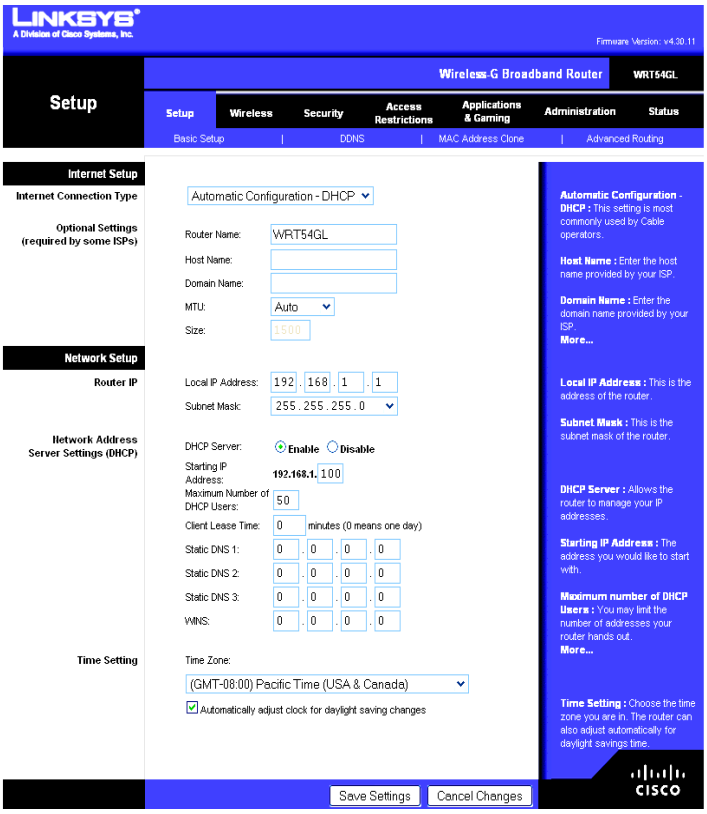


Fig. 2.31 Pantalla principal del firmware Versión: v4.30.11

Fuente: Creación propia.

Para cambiar el firmware del router se realizó los siguientes pasos:

a. Se seleccionó la pestaña administración y se activó la opción Firmware upgrade.

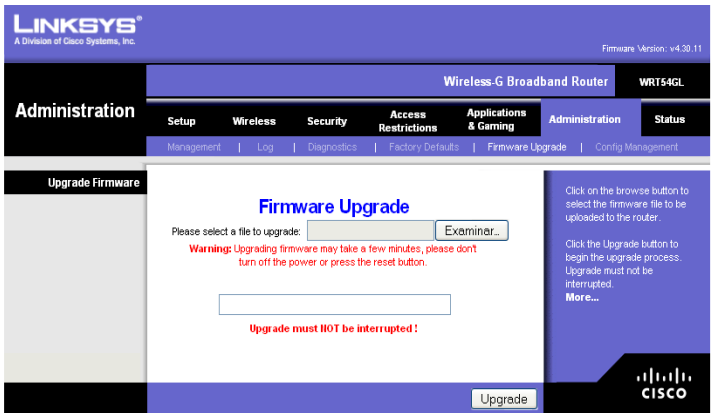


Fig. 2.32 Ventana de administración active firmware upgrade

Fuente: Creación propia

b. Con anterioridad se descargó de internet el *Firmware Hyperwrt _G_ Thibor 15c* y se guardó en el disco D. Se dio un clic en el botón examinar desplegándose la ventana de carga de archivos, se seleccionó y se abrió el software *Hyperwrt _G_ Thibor 15c*.

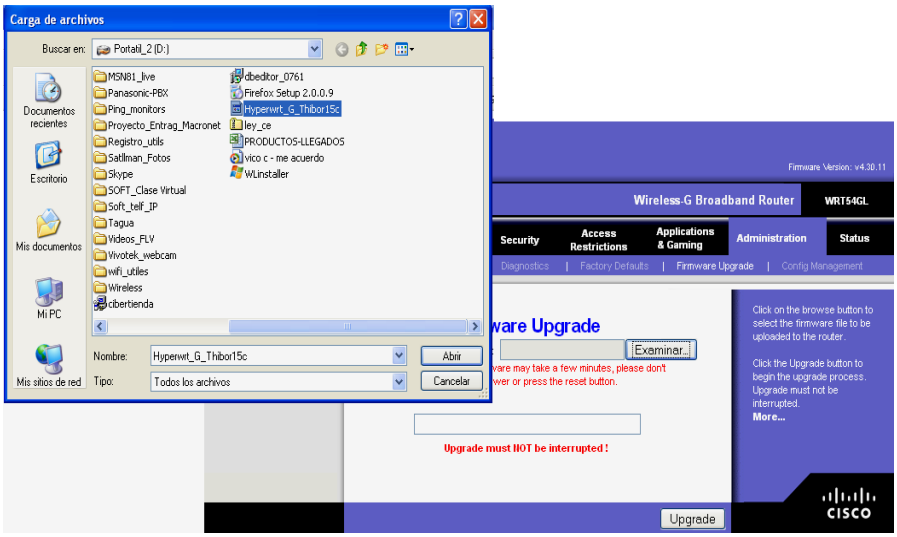


Fig. 2.33 Cargando el software Hyperwrt _G_ Thibor 15c

Fuente: Creación propia

c. Se pulsó *Upgrade* y se esperó que se cargue el Firmware, no se debe interrumpir la ejecución de este proceso porque se puede agraviar el equipo, el proceso duró unos minutos y se observó como avanza la ejecución.

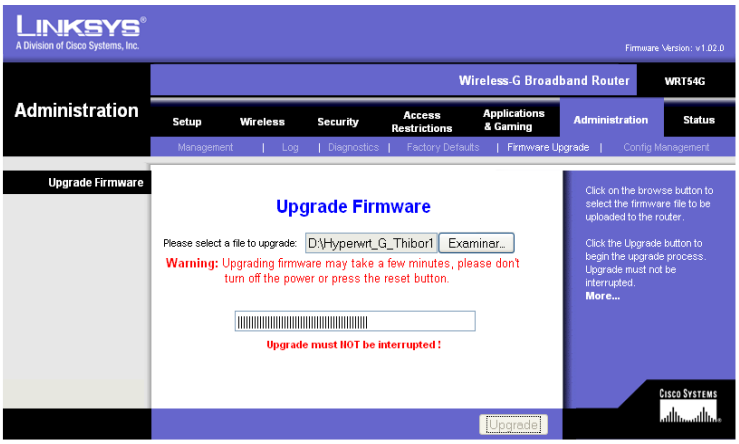


Fig. 2.34 Esperando la culminación del proceso

Fuente: Creación propia

d. Terminado el proceso, se desplegó la siguiente pantalla se presionó continúe y se reinició el router con el nuevo Firmware versión: v4.71.1. Hyperwrt 2.1b1+ Thibor 15c.

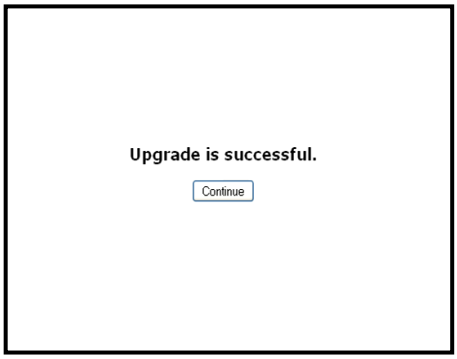


Fig. 2.35 Terminación del proceso

Fuente: Creación propia

e. Se observó el Firmware versión: v4.71.1. Hyperwrt 2.1b1+ Thibor 15c.

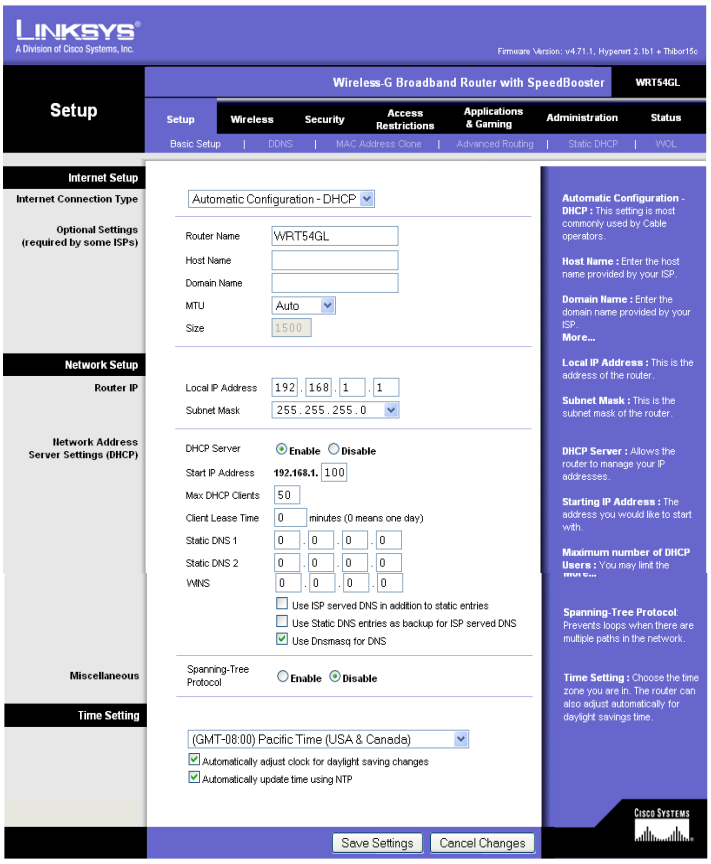


Fig. 2.36 Pantalla del nuevo Firmware versión: v4.71.1. Hyperwrt 2.1b1+ Thibor 15c

Fuente: Creación propia

2.3.3 Configuración de los routers inalámbricos Linksys WRT 54 GL v1.1.

Se realizó la configuración de los routers en el laboratorio del Dr. Henry Vallejo ubicado en las calles 7 de Mayo y 10 de Agosto. Se utilizó las direcciones IP: 192.168.1.1 para el equipo base y 192.168.1.2 para el equipo terminal.

Configuración del equipo base

Se activó la pestaña Wireless, en la opción Basic Wireless Settings se seleccionó las siguientes opciones:

Wireless Mode: *Access Point + WDS*; Wireless Netwok Mode: *Mixed*, se seleccionó esta opcion para trabajar con los estándares 802.11b a 11Mbps y 802.11g a 54 Mbps Wireless Network Name (SSID): Base; Wireless Channel: *11-2.462 GHz* se selecciónó el canal que este libre para evitar interferencia; Wireless SSID Broadcast: *Disable.*

En Mode: *Link with the following;* Remote Bridges*:29: D1:1E:FD: 00:21*; está es la MAC Wireless del equipo al que se enlaza al "Terminal".

Dentro de Wireless se seleccionó: Advanced Wireless Settings en el que se eligió las siguientes opciones: las trece primeras opciones mantienen sus valores y las siguientes cambiaron su configuración; Rx Antena: *Rigth*; Tx Antena: *Rigth*, Transmit Power: *Manual* y se aumentó la potencia del radio a *100 mV*.

Configuración del equipo terminal

Wireless Mode: *Access Point + WDS*; Wireless Netwok Mode: *Mixed*; Wireless Network Name (SSID): terminal; Wireless Channel: *11-2.462 GHz*, el equipo base y terminal fueron configurados en el mismo canal para el enlace; Wireless SSID Broadcast: *Disable.*

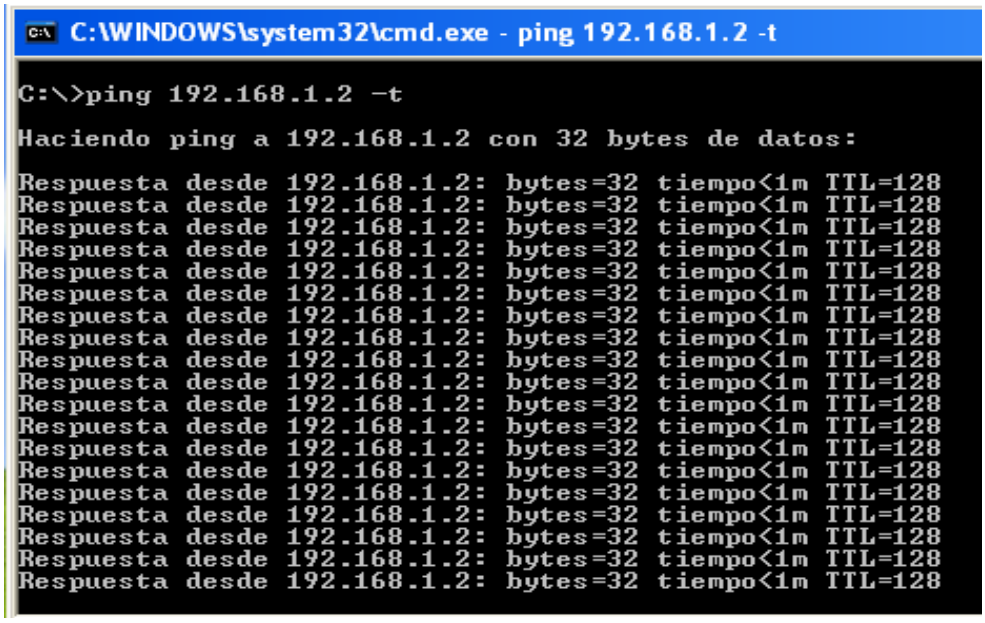
En Mode: *Link with the following;* Remote Bridges*: 00:1D:7E:18:99:C4*; está es la MAC Wireless del equipo al que se enlaza a la "Base".

Dentro de Wireless se activó Advanced Wireless Settings se seleccionó las siguientes opciones: las trece primeras opciones se mantienen y las siguientes cambiaron su configuracion; Rx Antena: *Rigth*; Tx Antena: *Rigth*, Transmit Power: *Manual* y se aumentó la potencia del radio a *100 mV*.

2.3.4 Pruebas de laboratorio de las antenas direccionales de Bi-Quad con los routers inalámbricos Linksys

Finalizada la configuración de los dos equipos, se conectó el pigtale, un extremo a la antena direccional y el otro al router inalámbrico; se colocó las antenas de tal manera que exista línea de vista directa entre los dos equipos, se realizó las pruebas de laboratorio obteniendo resultados satisfactorios. Se ejecutó las pruebas con la herramienta Ping; del router "Base" al router "Terminal" y viceversa los resultados se observan a continuación.

Router base al router terminal

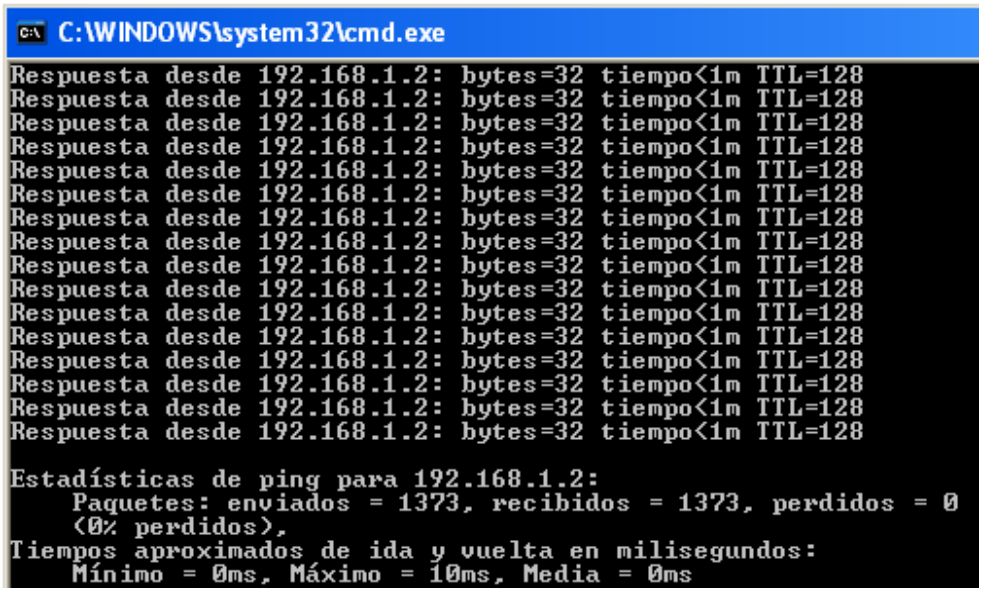


```
C:\>ping 192.168.1.2 -t

Haciendo ping a 192.168.1.2 con 32 bytes de datos:

Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
```

Fig. 2.37 Ping de la dirección 192.168.1.1 a la 192.168.1.2

Fuente: Creación propia

Continuación de la ejecución del comando ping router base al router terminal



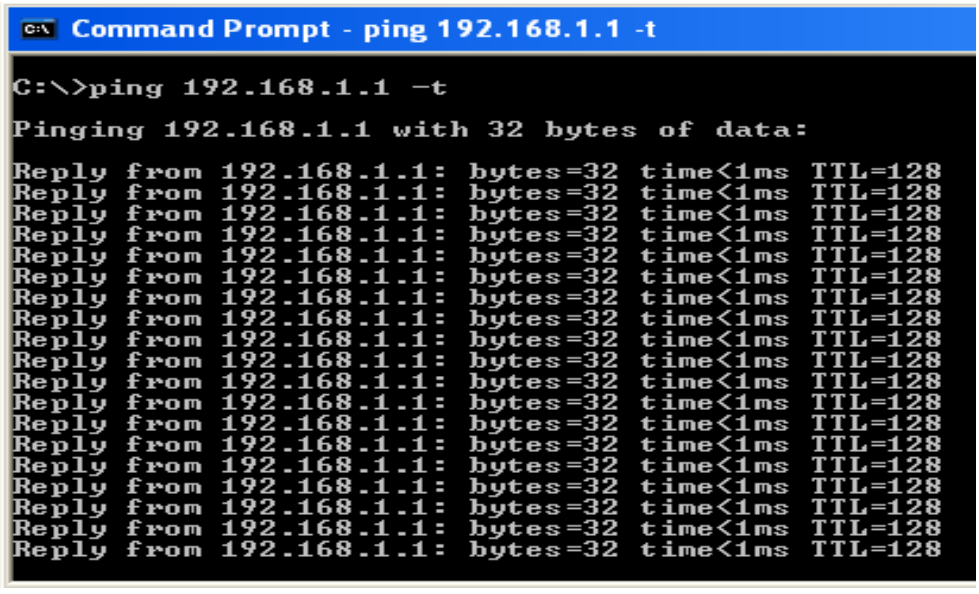
```
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 1373, recibidos = 1373, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 10ms, Media = 0ms
```

Fig. 2.38 Terminación del proceso

Fuente: Creación propia

No existió ninguna interferencia en la transmisión de datos se mantuvo el enlace.

Router terminal al router base

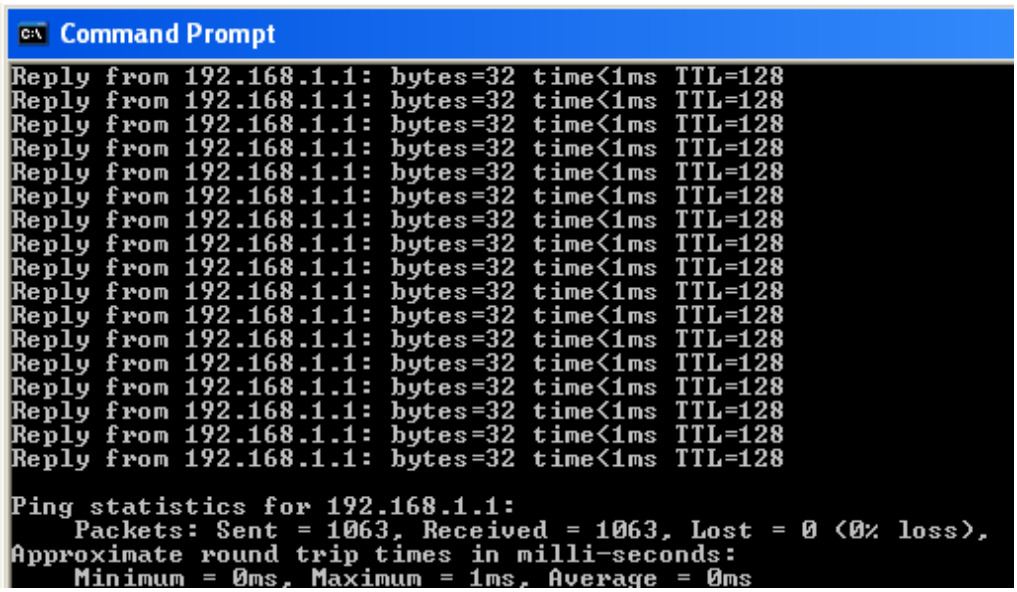


```
C:\>ping 192.168.1.1 -t

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
```

Fig. 2.39 Ping de la dirección 192.168.1.2 a la 192.168.1.1

Fuente: Creación propia

Continuación de la ejecución del comando ping router terminal al router base



```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 1063, Received = 1063, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fig. 2.40 Terminación del proceso

Fuente: Creación propia

Se obtuvo el mismo resultado en el otro extremo.

2.3.5 Pruebas de campo de las antenas direccionales de Bi-Quad con los routers inalámbricos Linksys.

Una vez construidas las antenas direccionales se ejecutó las pruebas de campo, se realizó a una distancia de 1km desde el centro histórico “Indio Guaranga” ubicado al noroeste de la ciudad hacia el edificio del “Sindicato de Chóferes de Bolívar” ubicado en las calles Sucre y García Moreno.

Se estabilizó las antenas colocándolas en pedestales, se conectaron los equipos en los dos puntos y se direccionó la antena del punto base “Indio Guaranga”, a la antena ubicada en la terraza del edificio del “Sindicato de Chóferes” punto Terminal con la ayuda de los binoculares.

Estas pruebas se las realizó con la dirección del Dr. Henry Vallejo.

Fig. 2.41 Estabilización de la antena base
Fuente: Creación propia

Fig. 2.42 Direccionamiento a la antena terminal
Fuente: Creación propia

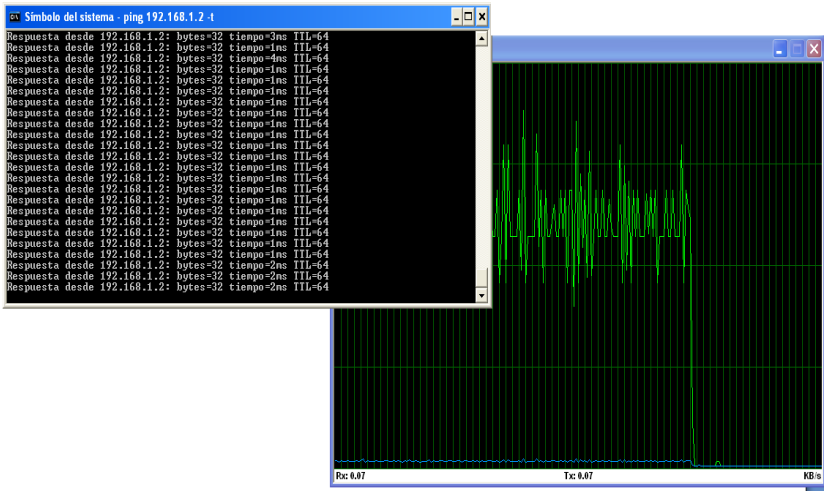
Fig. 2.43 Estabilización de la antena terminal
Fuente: Creación propia

Fig. 2.44 Direccionamiento a la antena Base
Fuente: Creación propia

Fig. 2.45 Dirección del Dr. Henry Vallejo
Fuente: Creación propia

Se demostró el alcance, el tiempo de respuesta y la tasa de transferencia de las antenas utilizando los programas RXTX32 y el PING. Se dio un ping a la dirección 192.168.1.2 del router terminal, y de igual manera a la dirección 192.168.1.1 del router base, hay que recalcar que esta configuración fue solo para la ejecución de las pruebas de campo.

Se ejecutó el programa RxTx32 el cual permitió ver los paquetes recibidos y transmitidos en un intervalo de tiempo.



```
Respuesta desde 192.168.1.2: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=2ms TTL=64
```

Fig. 2.46 Ping a la dirección 192.16.1.2 desde el Indio Guaranga

Fuente: Creación propia

Establecida la conexión se compartió un video del equipo terminal al equipo base y se observó que la reproducción del video era en tiempo real y sin ninguna interrupción.

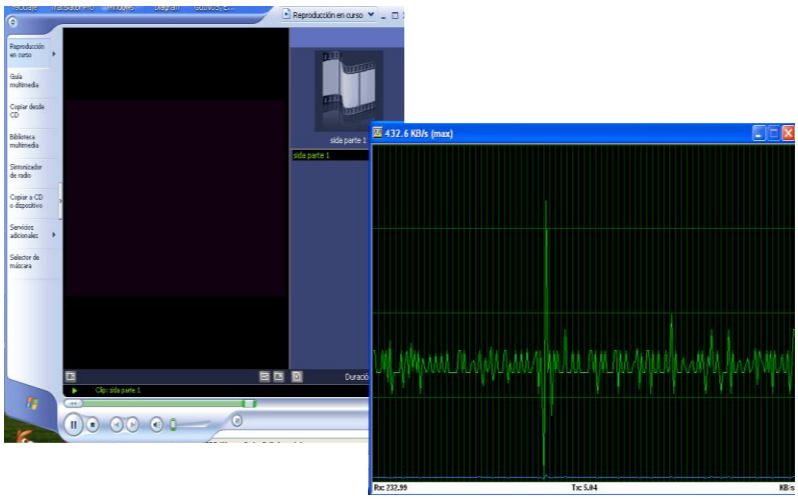


Fig. 2.47 Reproducción de un video compartido desde el Terminal a la Base

Fuente: Creación propia.

Con estas pruebas se ratificó que los routers y las antenas transmiten a 1km de distancia, superando las expectativas.

Se aprovechó la infraestructura del enlace, para lo cual se construyó una antena omnidireccional de 8 dBi, se requirió los siguientes materiales: Conector N chasis, tubo de cañería de cobre de 3/8 mm, tubo capilar de 1/12, cable de cobre #16, calibrador, regla milimetrada, arco de sierra, pernos, diagonal, pinza, cautín, estaño, pomada para soldar, masilla epóxica, tubo PVC eléctrico, silicón epóxica, silicón en barra, alicate, estilete, pelador de cable, loctite, pistola para tubo de silicón y lima.

2.3.6 Pasos para la Construcción de la Antena Omnidireccional

1. Se cortó las cuatro puntas del conector y se limó hasta dejarlo libre de limallas.

Fig. 2.48 Conector N chasis normal y limado
Fuente: Creación propia.

2. Se cortó 9 segmentos de tubo capilar: 8 de 5.60 cm y 1 de 6.15 cm; se cortó la cañería en 1 segmento de 3 cm. Se cortó 8 segmentos de cable de cobre y se realizó bobinas de 3 espirales con un ancho de 0.6 cm, con ayuda de un tornillo para formar el espiral.

Kit de elementos de la antena omnidireccional de 8dBi.

Fig. 2.49 Kit de elementos de la antena omnidireccional de 8dBi.

Fuente: Creación propia

3. Se soldó el segmento del tubo capilar de 6.15 cm de largo en el pin del conector, utilizando el cautín, estaño y pomada de suelda.

Fig. 2.50 El segmento de 6,15 cm soldado al pin del conector

Fuente: Creación propia

4. Se colocó la cañería de cobre de 3cm al conector y se soldó sobre la base (negativo) del mismo.

Para lo cual se coloco estaño en el conector y en el tubo capilar para soldar.

Fig. 2.51 La cañería de 3 cm soldada a la base negativa del conector
Fuente: Creación propia.

5. Se soldó las bobinas y los tubos capilares obteniendo segmentos de 9.8 cm.

Fig. 2.52 Bobinas y tubos capilares
Fuente: Creación propia

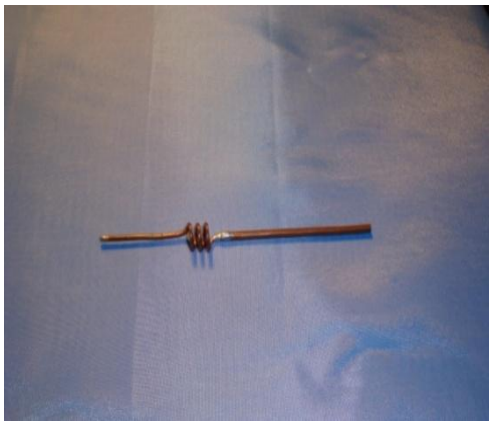


Fig. 2.53 Segmento de 9.8 cm de largo
Fuente: Creación propia

6. Se soldó 8 segmentos en serie, para terminar la antena.

Fig. 2.54 Los ocho segmentos soldados en serie

Fuente: Creación propia

7. Se dio rigidez a las bobinas rellenando con silicón.

Fig. 2.55 Relleno de bobinas

Fuente: Creación propia

1. Se colocó masilla epóxica al conector y al tubo capilar para asegurar la suelda.

Fig. 2.56 Preparación de la masilla epóxica

Fuente: Creación propia

Fig. 2.57 Colocación de la masilla epóxica

Fuente: propia

2. Se cortó el tubo PVC eléctrico de 80 cm de longitud, se limó sus extremos para eliminar impurezas.

Fig. 2.58 Cortada y limada del tubo PVC

Fuente: Creación propia

3. Se introdujo metió la antena omnidireccional en el tubo PVC y se rellenó con silicón epóxica dando rigidez a la misma y protegiéndola del medio ambiente.

Fig. 2.59 Introducción la antena en el tubo PVC
Fuente: Creación propia

Fig. 2.60 Colocar silicón epóxica
Fuente: Creación propia

4. Antena omnidireccional terminada.

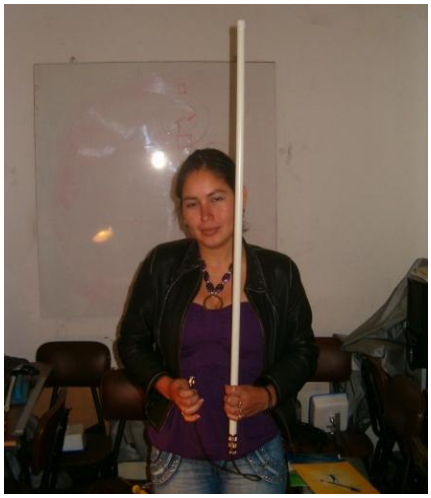


Fig. 2.61 Antena omnidireccional
Fuente: Creación propia

2.3.7 Pruebas de campo de la antena omnidireccional con el router inalámbrico Linksys

Una vez elaborada la antena omnidireccional se realizó las pruebas de campo dentro de los predios de la Universidad Estatal de Bolívar, tomando en cuenta distancias de 30m,

50m, 60m, 100m y de 150m a la redonda desde el edificio del Rectorado donde se colocó la antena omnidireccional. La potencia de las antenas se verificó con el programa Network Stumbler (Netstumbler), de los cuales se obtuvieron los siguientes resultados.

1) Prueba de la antena omnidireccional a los 30m.

Fig. 2.62 Terraza del edificio del Rectorado

Fuente: Creación propia

Fig. 2.63 Captura de datos a los 30m

Fuente: Creación propia

Resultado obtenido con el Netstumbler a los 30m.

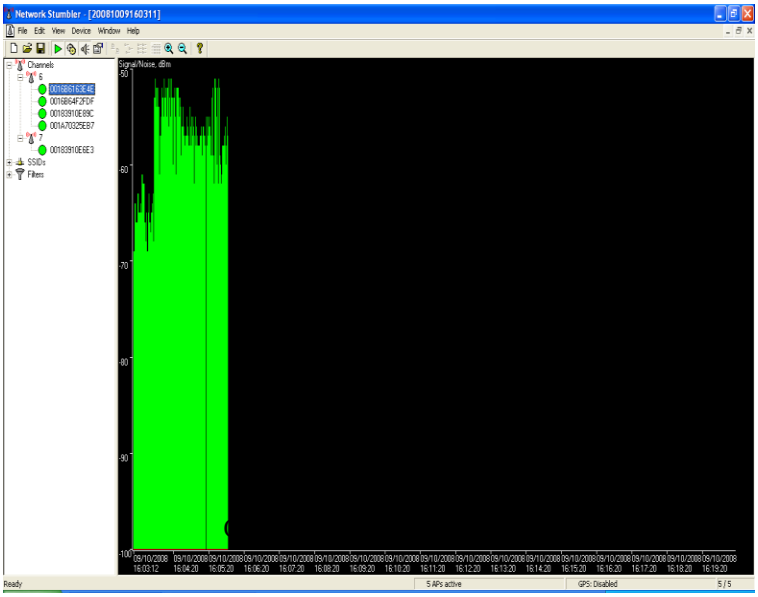


Fig.2.64 El resultado obtenido de la antena omnidireccional a los 30m fue de - 60 a - 50dBm.

Fuente: Creación propia

2) Prueba de la antena omnidireccional a los 50m.

Fig.2.65 Captura de datos a los 50m.

Fuente: Creación propia

Resultado obtenido con el Netstumbler a los 50m.

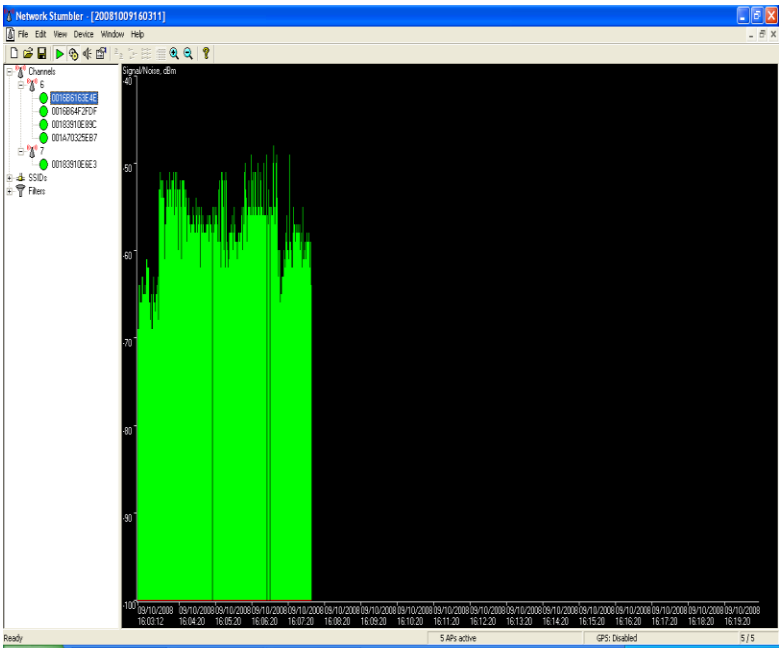


Fig. 2.66 El resultado obtenido de la antena omnidireccional a los 50m fue de – 58 a -50dBm.

Fuente: Creación propia

3) Prueba de la antena omnidireccional a los 60m.

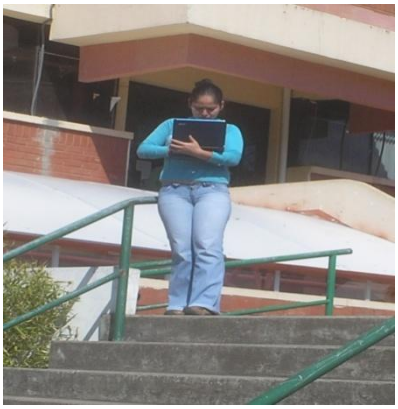


Fig.2.67 Captura de datos a los 60m.

Fuente: Creación propia

Resultado obtenido con el Netstumbler a los 60m.

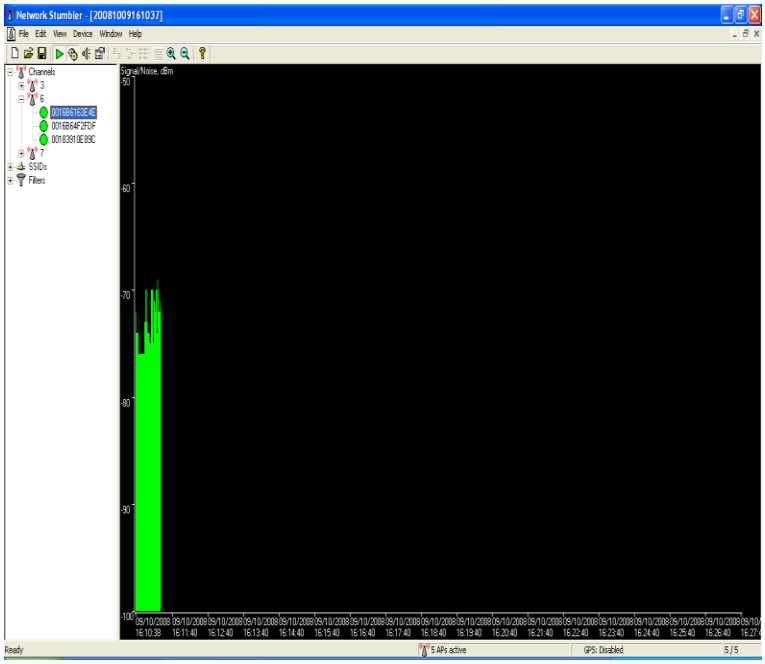


Fig.2.68 El resultado obtenido de la antena omnidireccional a los 60m fue de -70dBm.

Fuente: Creación propia

4) Prueba de la antena omnidireccional a los 100m.

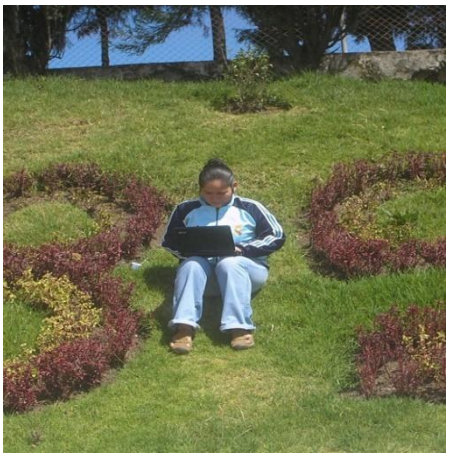


Fig.2.69 Captura de datos a los 100 m.

Fuente: Creación propia

Resultado obtenido con el Netstumbler a los 100m.

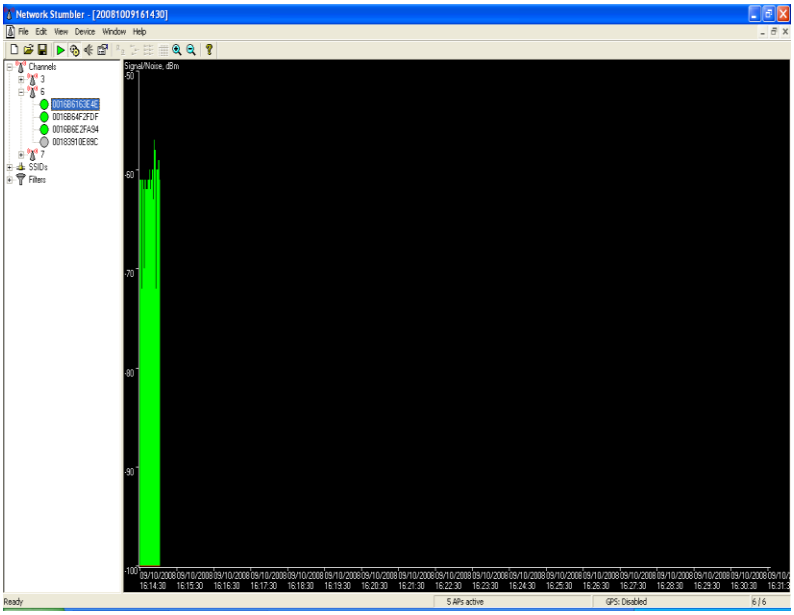


Fig. 2.70 El resultado obtenido de la antena omnidireccional a los 100m fue de - 60 dBm.

Fuente: Creación propia

5) Prueba de la antena omnidireccional a los 150m.

Fig. 2.71 Captura de datos a 150m.

Fuente: Creación propia.

Resultado obtenido con el Netstumbler a los 150m.

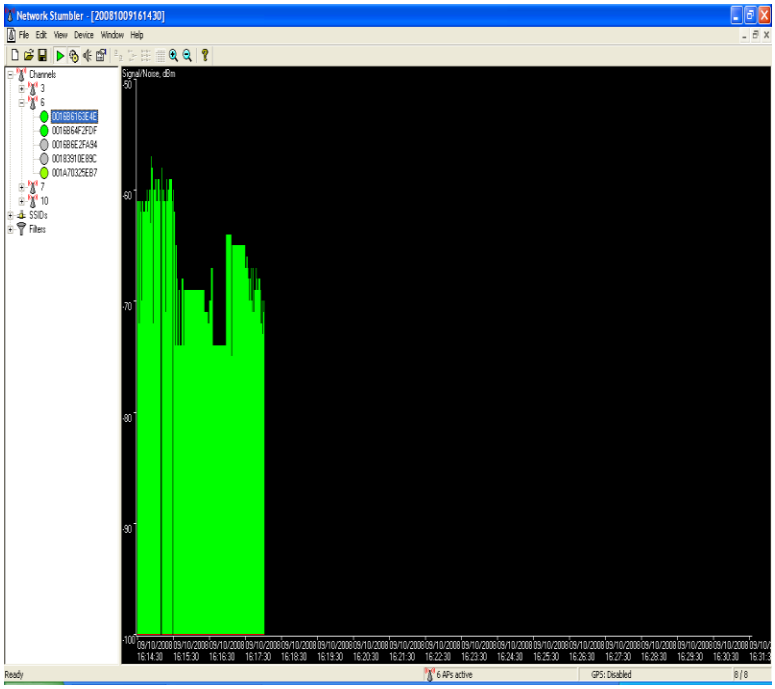


Fig. 2.72 El resultado obtenido de la antena omnidireccional a los 150m fue de – 70 a - 60 dBm.

Fuente: Creación propia

Concluidas las pruebas de la antena omnidireccional se determinó que esta antena cubre el área de cobertura estimada para los Hot-Spots.

2.4 IMPLEMENTACIÓN

Realizadas las pruebas de las antenas direccionales se construyeron dos antenas mas para el enlace. Además se protegió las antenas direccionales del medio ambiente colocándolas en cajas plásticas realizando los siguientes pasos:

a. En el centro de la caja plástica se realizó un agujero con la broca #12 utilizando el taladro, y se limó el contorno para eliminar impurezas.

Fig. 2.73 Realización del agujero y eliminación de impurezas

Fuente: Creación propia.

b. Se remachó una placa de baquelita con el brazo metálico; el brazo metálico consta de dos segmentos de tubos cuadrados, 1 de 7.5 cm de longitud que va a la caja plástica y el otro de 15.3 cm que va a la platina unidos a través de un bocín (tornillo de mariposa).

Fig. 2.74 Brazo metálico remachado a la caja plástica

Fuente: Creación propia.

c. Se pintó con pintura blanca el interior de la caja.

Fig. 2.75 Pintada de la caja
Fuente: Creación propia.

d. Se colocó la antena en polarización vertical dentro de la caja plástica. La antena fue fijada a la caja con la ayuda de silicona en barra colocada en las esquinas de la placa y se cerró herméticamente la caja con silicona.

Fig. 2.76 Antena polarizada verticalmente.
Fuente: Creación propia.

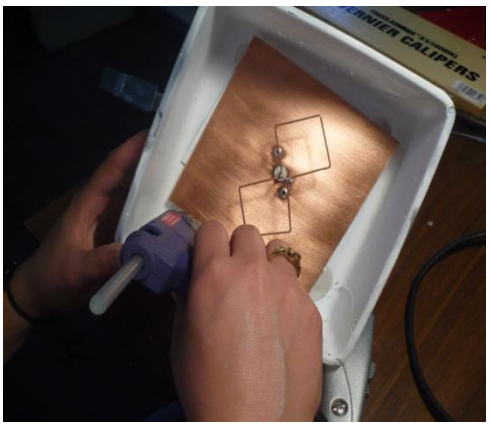


Fig. 2.77 Colocación de silicón
Fuente: Creación propia.

2.4.1 COLOCACIÓN DE LAS PLACAS ELECTRÓNICAS EN LAS CAJAS HERMÉTICAS.

1. Se retiró las seguridades de las cajas del router y se extrajo sus tarjetas electrónicas y se las colocó en las cajas herméticas.

Fig. 2.78 Extracción de la tarjeta electrónica

Fuente: Creación propia.

2. En cada caja hermética se colocó dos tarjetas electrónicas separadas por tres bocines (postes plásticos con tornillos), la placa inferior es el router y la superior es el Access point.

Fig. 2.79 Interior de la caja hermética.

Fuente: Creación propia

3. Se fijó con silicón las fuentes de corriente en la parte superior de las placas electrónicas manteniendo una distancia considerable.

Fig. 2.80 Fijación de las fuentes de corriente

Fuente: Creación propia

4. En la caja hermética se incorporaron los cables de datos, corriente eléctrica y dos pigtales uno que va del router a la antena directiva y el otro del Access point a la antena omnidireccional, estos procesos se realizaron solo en los puntos de La Casona Universitaria y La Casa Regional de Bolívar.

   En el Obispado se colocó tres pigtales; dos que van del router a las antenas directivas, una direccionada a la Casona Universitaria y otra a la Casa Regional de Bolívar, el tercero del Access point a la antena omnidireccional.

   El cable de corriente, el de datos y los pigtales previamente se introdujeron en una manguera espiral para protegerlos del medio ambiente.

   La longitud del cable de datos y eléctrico para la Casona Universitaria fue de 25m, en el Obispado de 15m, y en la Casa Regional de Bolívar fue de 70m.

   Se colocó los cables en la manguera espiral y se introdujo en la caja hermética, se procuró no lastimar los cables con el filo de la manguera por ello se los cubrió con taipe.

Se observa la introducción de la manguera espiral en la caja hermética.

Fig. 2.81 Introducción de la manguera espiral en la gaveta metálica

Fuente: Creación propia

5. Se conectó el cable de corriente a las placas electrónicas y los cables de datos; el primer cable de datos va desde el segundo puerto del switch que se encuentra en la oficina de los voluntarios norteamericanos del Programa World Teach a la WAN del router, este procedimiento solo se lo realizó en la Casona Universitaria

   Los siguientes pasos se realizaron en los tres puntos; se colocó un patch cord directo de 15 cm de longitud del primer puerto de la LAN del router hacia la WAN del Access point y otro de un puerto LAN del router conectado a una computadora portátil para el monitoreo y mantenimiento de la red de datos.

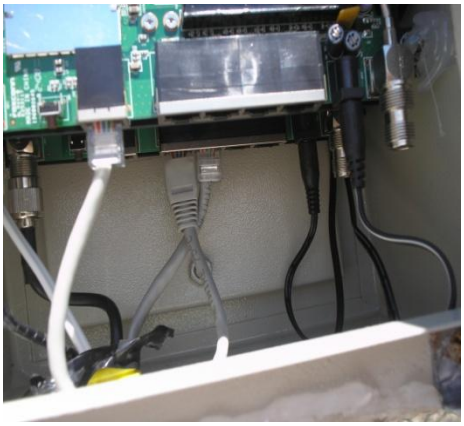


Fig. 2.82 Conexión interna del Router al Access Point

Fuente: Creación propia

6. Las cajas herméticas se cerraron con silicón en barra, en la parte de la manguera espiral se protegió con autofundente y silicón evitando principalmente el ingreso del agua; se conectó los pigtales a la antena direccional y omnidireccional, de igual manera los conectores de las antenas se protegieron con autofundente y silicón.

Fig. 2.83 Protección del conector de la antena

Fuente: Creación propia

Fig. 2.84 Protección de la caja hermética

Fuente: Creación propia

La antena direccional, omnidireccional y la caja hermética formaron el equipo que se instaló en cada punto.

2.4.2 INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS EN LA TORRE Y MÁSTILES

1. Para la instalación del primer punto Casona Universitaria no se requirió de un mástil porque existe una torre prefabricada de 15 m, donde se encuentra un tubo galvanizado de 60 cm. atornillado a la torre y este contiene dos placas soldadas donde anteriormente se encontraba la caja hermética con un Access point Linksys WRT54G perteneciente a la Universidad Estatal de Bolívar.

   En el tubo galvanizado se atornilló la caja hermética con una abrazadera metálica, arandelas de presión y tuercas, en el cuál también está sustentada la antena omnidireccional de 16 dBi de la U.E.B y está conectada por un pigtale al Access point.

La manguera espiral fue sujetada a la torre con amaras plásticas de 30 cm de longitud.

Fig. 2.85 Atornillación de la caja hermética

Fuente: Creación propia

Fig.2.86 Sujetación de la manguera espiral

Fuente: Creación propia

Se enchufó el cable eléctrico y el cable de datos se conectó a la computadora portátil, se esperó unos minutos hasta que el equipo esté listo y se procedió a configurar el primer punto:

Configuración del router Casona Universitaria.

Se ingresó al equipo a través del browser se selecciónó la pestaña Setup y se procedió a la configuración:

Static IP con las siguientes direcciones; Internet IP Address: *192.168.1.200*; Subnet Mask: *255.255.255.0*; Gateway: *192.168.1.1*; Static DNS 1: *200.107.60.58*; Static DNS 2: *200.107.10.62*; Router Name: *CasonaUEB*; Host Name: *CasonaUEB*.

Local IP Address: *192.168.2.1*; Subnet Mask: *255.255.255.0*; DHCP Server: *Disable*; Spanning Tree Protocol: *Disable*; Time Seting: *GMT-05-00 Indiana East, Colombia, Panama*; realizados estos cambios se guardó *Save Settings* .

Se esperó que el equipo procese los cambios.

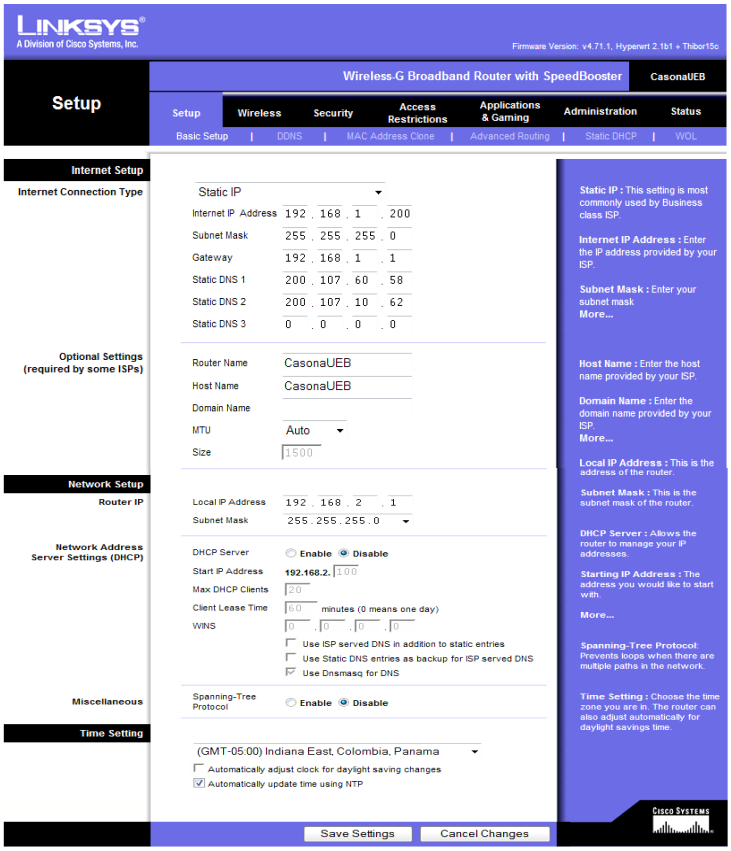


Fig. 2.87 Configuración del Setup

Fuente: Creación propia.

Seguidamente se activó la pestaña Wireless, en la opción Basic Wireless Settings se seleccionaron las siguientes opciones:

Wireless Mode: *Access Point + WDS*; Wireless Netwok Mode: *Mixed*; Wireless Network Name (SSID):*CASONAUEB*; Wireless Channel: *11-2.462 GHz*; Wireless SSID Broadcast: *Disable.*

En Mode: *Link with the following;* Remote Bridges*: 00:21:29: D1:1E:FD*; está es la MAC Wireless al que se enlaza el equipo (REPETIDORUEB).

Se dio clic en *Save Settings* para guardar los cambios.

Fig. 2.88 Configuraión de la pestaña Wirreles

Fuente: Creación propia.

En Advanced Wireless Settings las trece primeras opciones se mantienen Rx Antena: *Rigth*; Tx Antena: *Rigth*, Transmit Power: *Manual* y se incrementó la potencia del radio a *150 mV*, y se guardó *Save Settings*.

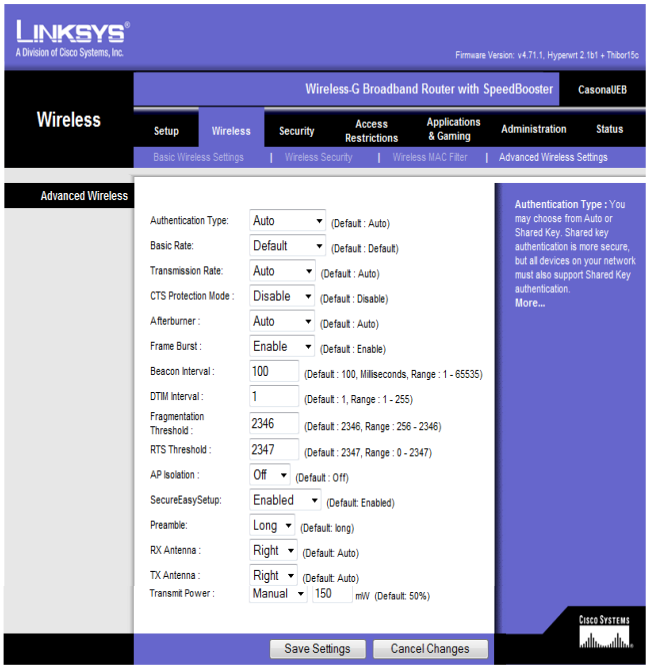


Fig. 2.89 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

En la pestaña Administración se seleccionó la opción Management, donde se procedió a cambiar la contraseña para el ingreso al equipo con su respectiva confirmación (routercasona); se activó las siguientes opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*, SSHD: *Disable*, y se guardó dando clic en *Save Settings*.

Fig. 2.90 Administración de contraseña de ingreso

Fuente: Creación propia.

En la pestaña Status en la opción Wireless, se observa las siguientes características: MAC Address: 00:1D:7E:18:99:C4 (MAC con la que se enlaza el otro equipo); Mode: Mixed; SSID: CASONAUEB; DHCP Server: Disable; Chanel: 11; Encrytion Funtion: Disable.

Si se realiza alguna modificación dar clic en Refresh para observar los cambios.

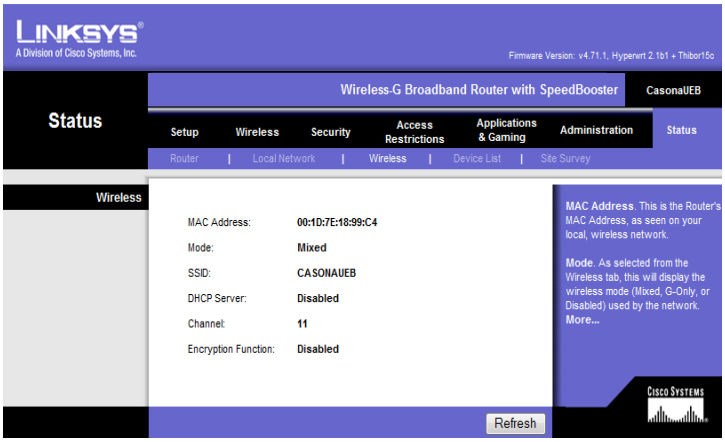


Fig. 2.91 Datos configurados del equipo

Fuente: Creación propia.

En la pestaña Status en la opción Site Survey se observó los SSIDS, las MAC Address, el canal de frecuencias y la potencia que tienen los equipos inalámbricos que están operativos.

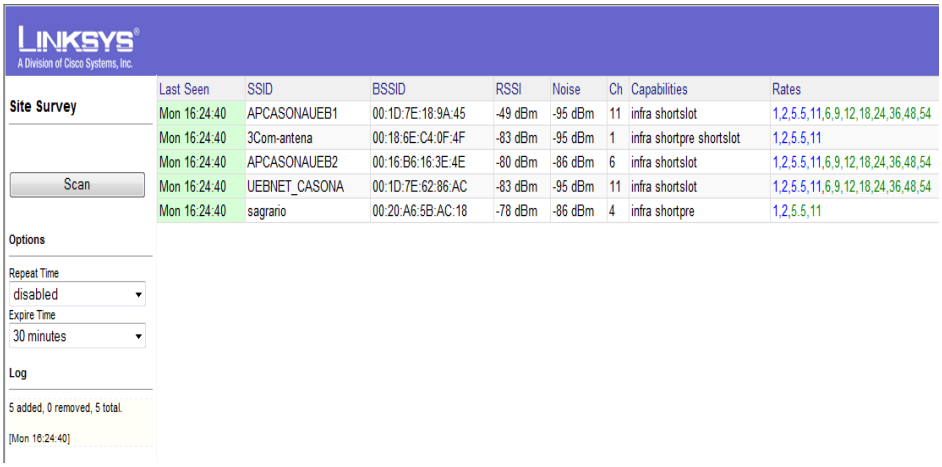


Fig. 2. 92 Ventana de equipos operativos

Fuente: Creación propia.

Access point Casona Universitaria

Se ingresó al equipo a través de browser, en Setup se configuró: Static IP con las siguientes direcciones; Internet IP Address: *192.168.2.10*; Subnet Mask:

255.255.255.0; Gateway: *192.168.2.1*; Static DNS 1: *200.107.60.58*; Static DNS 2: *200.107.10.62*; Router Name: *APCASONAUEB.*

Local IP Address: *192.168.3.1*; Subnet Mask: *255.255.255.0*; DHCP Server:*Enable*; Start IP Address: *192.168.3.100*; Max DHCP Clients: *20*, se puede aumentar el número de clientes pero no es recomendable ya que disminuyeria el ancho de banda; Client Lease Time: *60* minutes; Activamos: Use Dnsmasq for DNS; Spanning Tree Protocol: *Disable;* Time Seting: *GMT-05-00 Indiana East, Colombia, Panama*; una vez realizados estos cambios se guardó dando clic en *Save Settings*.

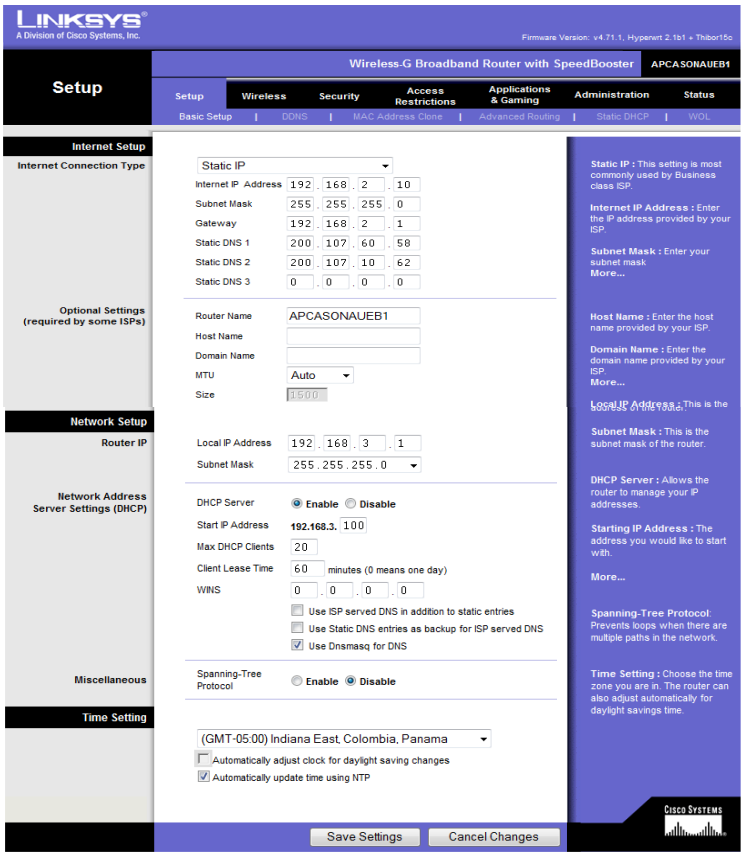


Fig.2.93 Configuración del Setup

Fuente: Creación propia.

En la opción Basic Wireless Settings de Wireless, se seleccionó las siguientes opciones: Wireless Mode: *Access Poin;* Wireless Netwok Mode: *Mixed*;

Wireless Network Name (SSID):*APCASONAUEB1*; Wireless Channel: 9-*2.462 GHz*; Wireless SSID Broadcast: *Enable*, y se guardó *Save Settings*.

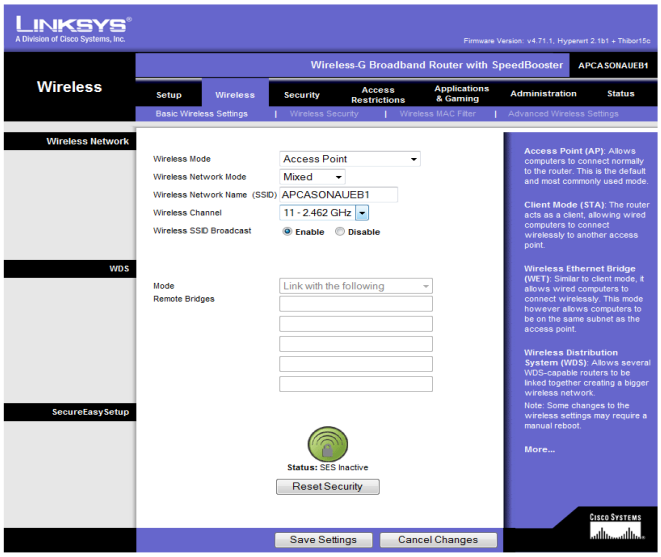


Fig. 2.94 Configuracion de la pesta;a wireless

Fuente: Creación propia.

En Advanced Wireless Settings las trece primeras opciones se mantienen. Rx Antena: *Right*; Tx Antena: *Right*, Transmit Power: *Manual* y se incrementó la potencia del radio a *100 mV*, se guardó *Save Settings*.

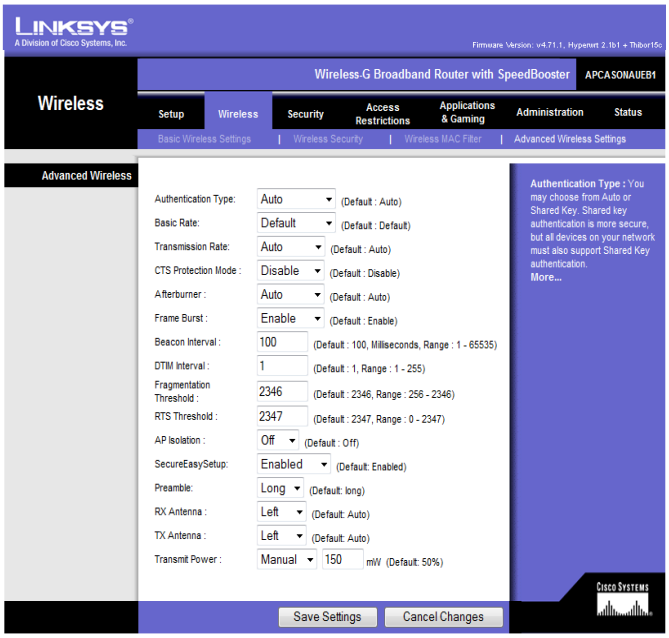


Fig. 2.95 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

En la pestaña Administración se seleccionó la opción Management, se procedió a cambiar la contraseña con la que se accede al equipo (apcasona) con su respectiva confirmación; se activó las siguientes opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*, Estabished state timeout; *600 (*seconds*);* Max Connections: *2048*; SSHD: *Disable;* Status Stopped: *Allow wireless Access;* y se guardó *Save Settings*.

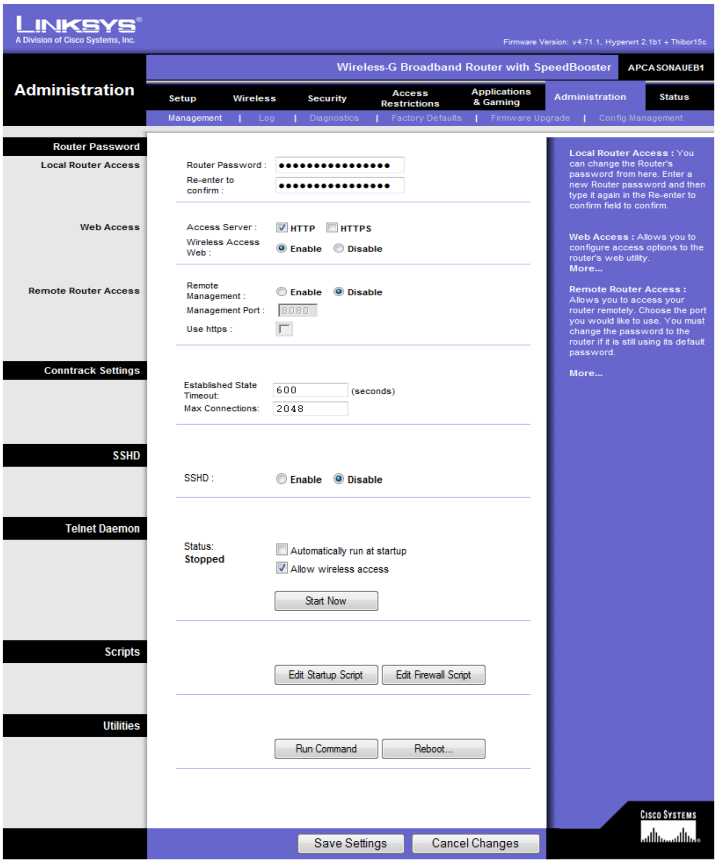


Fig. 2.96 Administracion de constrasena de ingreso

Fuente: Creación propia.

Dentro de Status se seleccionó Device List, donde podemos se observa todos los equipos conectados al Access Point.

Usuarios conectados

Device List
Refresh

IF	MAC Address	IP Address	Name	RSSI	Lease Expires
br0	00:1D:E0:4C:6A:CD	192.168.3.103	KattyLozano1	-91 dBm	0 days, 00:35:28
br0	00:23:4D:5D:10:CF	192.168.3.108	Luigui1	-91 dBm	0 days, 00:59:27
br0	00:21:63:90:BB:7F	192.168.3.110	MAROSVEVE1	-91 dBm	0 days, 00:52:51
br0	00:08:A1:A4:E4:80	192.168.3.100	MULTISYS-4F64D1	-87 dBm	0 days, 00:48:39
eth1	00:21:00:AF:05:69	192.168.3.117	Pc	-90 dBm	0 days, 00:50:08
br0	00:21:00:58:2D:35	192.168.3.111	UEB1	-92 dBm	0 days, 00:45:28
br0	00:19:D2:4C:8A:7A	192.168.3.104	XavierJimenez21	-86 dBm	0 days, 00:34:45
br0	00:17:3F:D2:C8:6D	192.168.3.105	galo	-85 dBm	0 days, 00:59:37
br0	00:14:A4:6E:21:E9	192.168.3.101	personal-96e38c	-87 dBm	0 days, 00:35:00
br0	00:22:B0:56:74:80	192.168.3.102	usuario-8b509b4	-84 dBm	0 days, 00:51:35
vlan1	00:1D:7E:18:99:C2	192.168.2.1			

Fig 2. 97 Ventana de usuarios

Fuente: Creación propia.

Para ver la conectividad del equipo se ingresó al símbolo del sistema (MS-DOS) y se dio un ping a la dirección del router 192.168.2.1 verificando el tiempo de respuesta.

La red inalámbrica se verificó mediante la conexión al Access point APCASONAUEB y se ingresó a Internet verificando la tasa de transferencia.

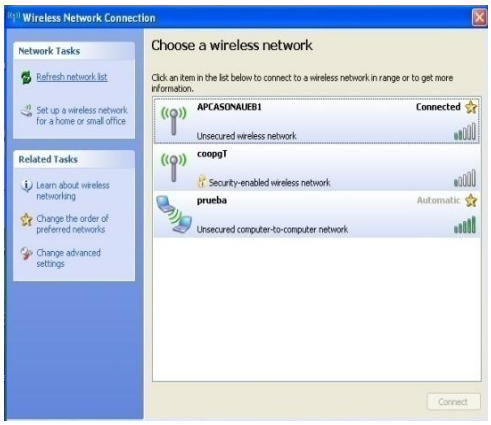


Fig. 2.98 Conectado al Access Point

Fuente: Creación propia

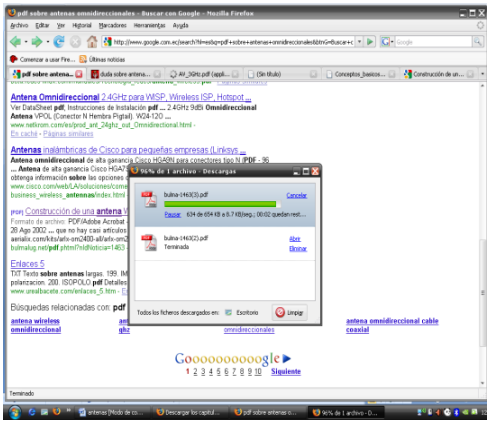


Fig. 2.99 Finalización de la descarga

Fuente: Creación propia

Primer punto instalado en la torre prefabricada que se encuentra en “La Casona Universitaria”.

Fig. 2.100 Primer punto Casona Universitaria

Fuente: Creación propia

2. Se instaló el segundo punto en el edificio del Obispado; se colocó un mástil de 3.20 m de longitud, un extremo se encajó en un pedestal metálico y en el otro se acondicionó el equipo, sujetando la caja hermética al mástil con una abrazadera metálica en U, tornillos, arandelas de presión y tuercas.

Fig. 2.101 Acondicionamiento de la caja hermética

Fuente: Creación propia

La antena omnidireccional se fijó en el extremo del mástil con abrazaderas metálicas en U, tornillos, tuercas y arandelas de presión.

Fig. 2.102 Fijación de la antena Omnidireccional
Fuente: Creación propia

Las antenas direccionales se las colocó en la parte inferior de la caja hermética sujetándolas con dos abrazaderas galvanizadas.

Fig. 2.103 Sujetación de la antena direccional
Fuente: Creación propia

Se colocó una abrazadera en U donde se sujetaron los tres tensores de alambre galvanizado los mismos que dieron firmeza al mástil. Además se colocó taipe en los trenzados del alambre galvanizado evitando la oxidación.

También se realizó cuatro perforaciones en el piso de concreto con el taladro y la broca #12 y se introdujo los tacos fisher y los tirafondos de esta manera se aseguro el mástil.

Fig. 2.104 Colocación de la abrazadera en U

Fuente: Creación propia

Fig. 2.105 Perforación del concreto

Fuente: Creación propia

Los rompe vientos formaron un triángulo isósceles; para lo cual se perforó el piso con el taladro y la broca #12 en los vértices del triángulo, se colocó los tacos fisher y los cáncamos, se equilibró el mástil con ayuda del nivel y los tensado de vientos.

Fig. 2.106 Colocación de los rompe vientos

Fuente: Creación propia

Instalado el segundo punto se direccionaron las antenas, una hacia La Casona Universitaria y la otra hacia La Casa Regional de Bolívar.

Fig. 2.107 Direccionar-Casona Universitaria

Fuente: Creación propia

Fig. 2.108 Direccionar-Casa Regional de B.

Fuente: Creación propia

Se enchufó el cable eléctrico y se conectó el cable de datos a la computadora portátil, se esperó unos minutos hasta que el equipo esté listo, y se procedió a configurar el primer punto:

Configuración del router Obispado

Se ingresó al equipo a través del browser y se procedio a configurar el ruoter inalámbrico:

Se seleccionó la pestaña Setup en la opción Basic Setup se realizó la configuración: En Automatic Configuration se elegió Automatic Configuration - DHCP; Router Name: *REPETIDORUEB*. Local IP Address: *192.168.2.2*; Subnet Mask: *255.255.255.0*; DHCP Server: *Disable*; Spanning Tree Protocol: *Disable*; Time Seting: *GMT-05-00 Indiana East, Colombia, Panama*;

Para guardar los cambios se dio clic *Save Settings*.

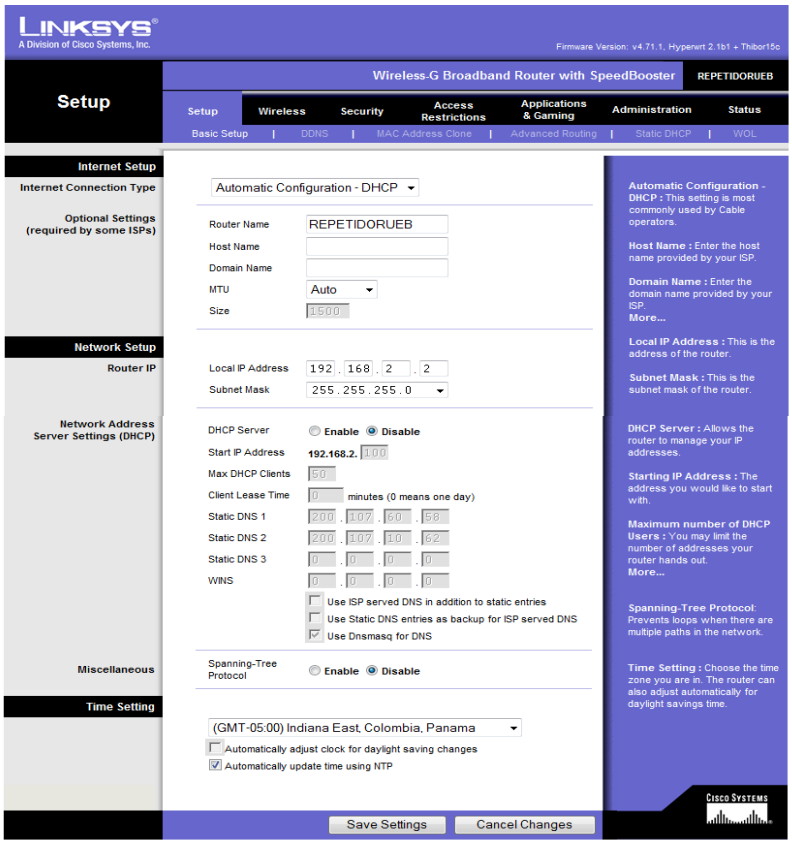


Fig. 2.109 Configuracion del Setup

Fuente: Creación propia.

Se activó la pestaña Wireless, en la opción Basic Wireless Settings se seleccionó las siguientes opciones: Wireless Mode: *Access Point + WDS*; Wireless Netwok Mode: *Mixed*; Wireless Network Name (SSID): *RepetidorUEB*; Wireless Channel: *11-2.462 GHz*; Wireless SSID Broadcast: *Disable.*

En Mode: *Link with the following;* Remote Bridges*: 00:1D:7E:18:99:C4 y 00:1D:7E:F8:22:C4* , estas son las direcciónes MAC Address Wireless de los equipos a los que se direccionan (CASONAUEB - EECAUEB) esta es la parte primordial para que funcione como repetidor.

Se dio clic en *Save Settings* para guardar los cambios.

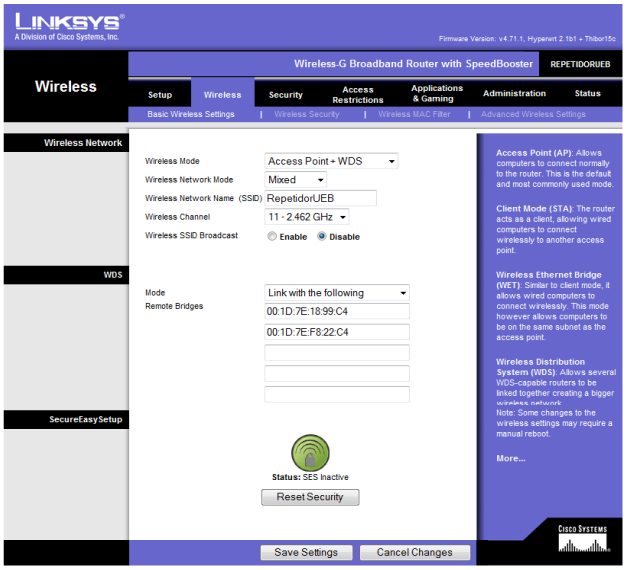


Fig. 2.110 Configuraión de la pestaña Wirreles

Fuente: Creación propia.

En Advanced Wireless Settings las trece primeras opciones se mantienen. Rx Antena: *Rigth*; Tx Antena: *Left*; Transmit Power: *Manual* y se incrementó la potencia del radio a *100 mV*; se guardó *Save Settings*.

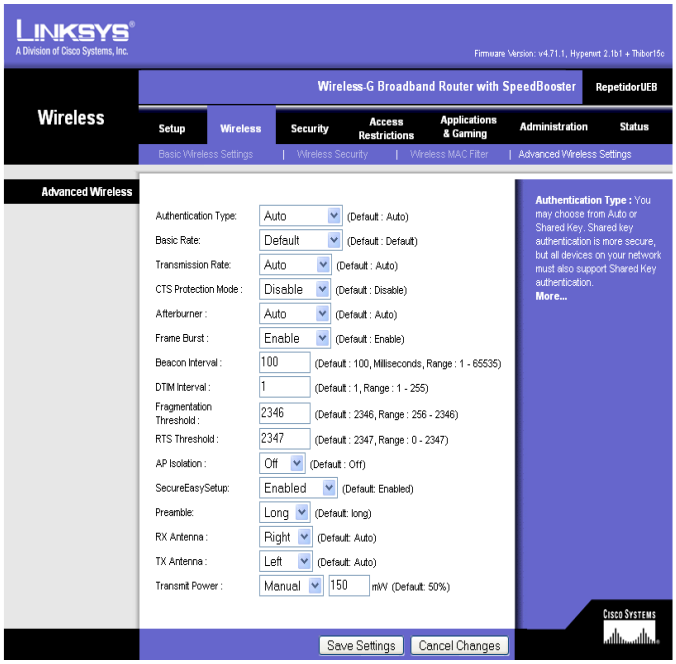


Fig. 2.111 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

En la pestaña Administración se seleccionó la opción Management, se procedió a cambiar la contraseña (routerobispado) con su respectiva confirmación; se activó las siguientes opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*, SSHD: *Disable;* Status Stopped: *Allow wireless Access;* y se guardó *Save Settings*.

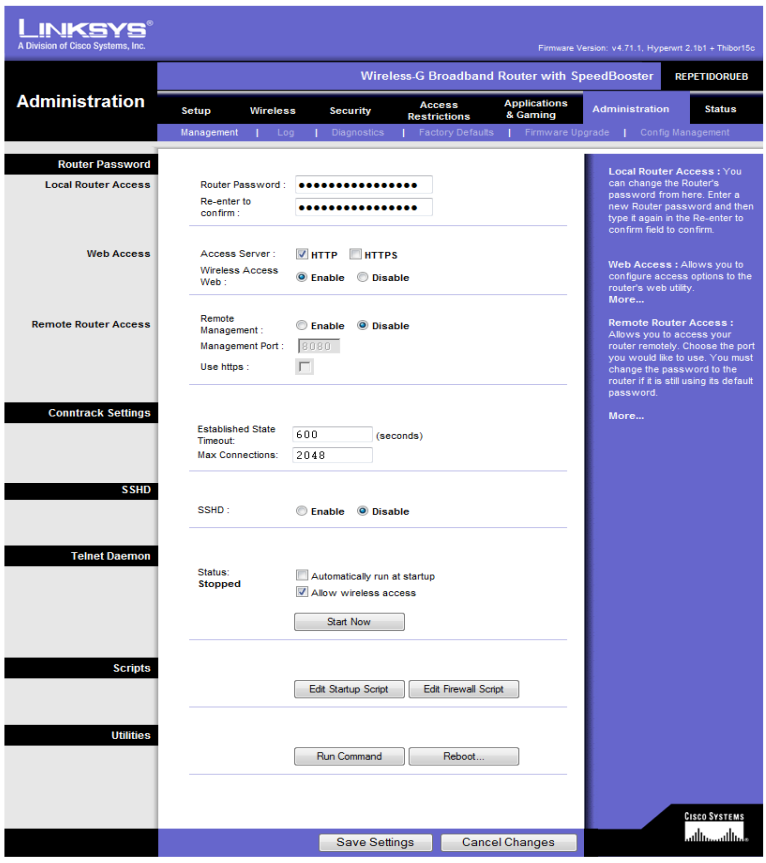


Fig. 2.112 Administración de contraseña de ingreso

Fuente: Creación propia.

Se seleccionó la pestaña Status dentro de esta se activó la opción Wireless, en esta ventana se observa las configuraciones que se han realizado en el equipo: MAC Address: 00:21:29:D1:1E: FBI; Mode: Mixed; SSID: RepetidorUEB; DHCP Server: Disable; Chanel: 11; Encrytion Funtion: Disable.

Si se realiza alguna modificación dar clic en Refresh.

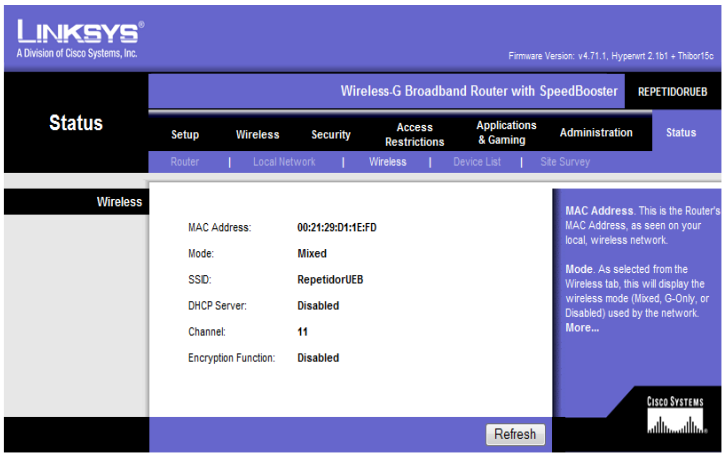


Fig. 2.113 Datos configurados del equipo

Fuente: Creación propia.

En Status en la opción Site Survey se observa los SSIDS, MAC Wireless, el canal de frecuencia y la potencia que tienen los equipos que están operativos.

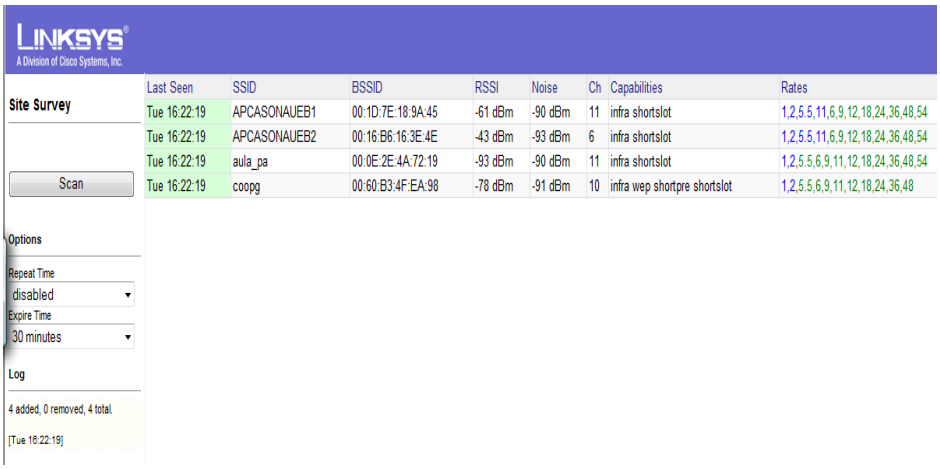


Fig. 2. 114 Ventana de equipos operativos

Fuente: Creación propia.

Access Point Obispado

El equipo WRT54G version v1.02.0 no permitió cambiar su Firmware, En la pestaña Setup se configuró: Static IP con las siguientes direcciones; Internet IP Address: *192.168.2.11*; Subnet Mask: *255.255.255.0*; Gateway: *192.168.2.1*; Static DNS 1: *200.107.60.58*; Static DNS 2: *200.107.10.62*;

Router Name: *APCASONAUEB2*. Local IP Address: *192.168.4.1*; Subnet Mask: *255.255.255.0*; DHCP Server:*Enable*; Start IP Address: *192.168.4.100*; Maximum Numbers of DHCP Users: *50*, se puede aumentar el número de clientes pero no se recomienda, disminuye el ancho de banda; Client Lease Time: *60* minutes; Activamos: *Use Dnsmasq for DNS*; Spanning Tree Protocol: *Disable;* Time Seting: *GMT-05-00 Indiana East, Colombia, Panama*; realizados los cambios dar clic en *Save Settings.*

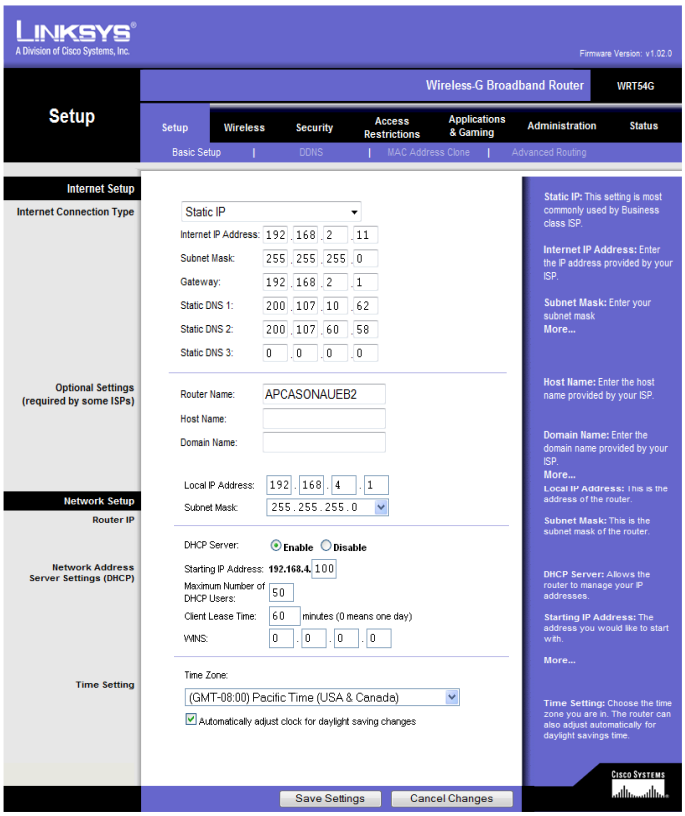


Fig. 2.115 Configuracion del Setup

Fuente: Creación propia.

Se activó la pestaña Wireless, en la opción Basic Wireless Settings se seleccionó las siguientes opciones: Wireless Mode: *Access Poin;* Wireless Netwok Mode: *Mixed*; Wireless Network Name

(SSID):*APCASONAUEB2*; Wireless Channel: *6 -2.462 GHz*; Wireless SSID Broadcast: *Enable*, y se guardó *Save Settings*.

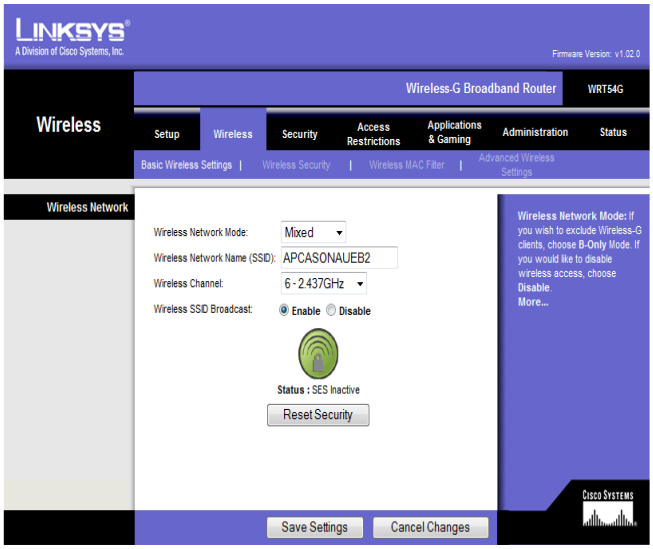


Fig. 2. 116 Configuración de la pestaña Wireless

Fuente: Creación propia.

En Advanced Wireless Setting, no se hizo ningún cambio el router Wireless-G Broadband marca Linksys no permite la actualización del Firmware.

Fig. 2.117 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

En Administración se seleccionó la opción Management, se cambió la contraseña de acceso al equipo (apobispado) con su respectiva confirmación; se activó las opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*; UPnP: Disable*;* y se guardó *Save Settings*.

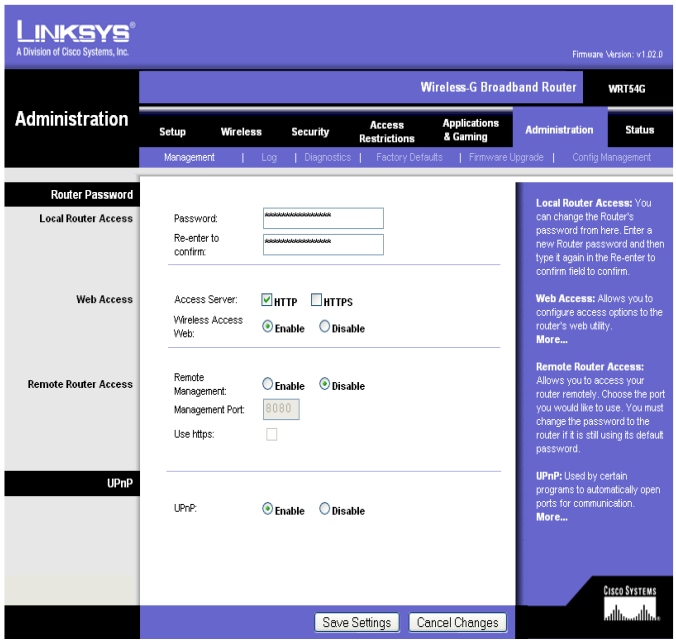


Fig. 2.118 Administracion de contraseña de ingreso

Fuente: Creación propia.

Status en la opción Wireless se observa las opciones; MAC Address: 00:16:B6:16:3E:4E; Mode: Mixed 11/54Mbps; SSID: APCASONAUEB2; DHCP Server: Enable; Chanel: 6; Encryption funtion: Disable.

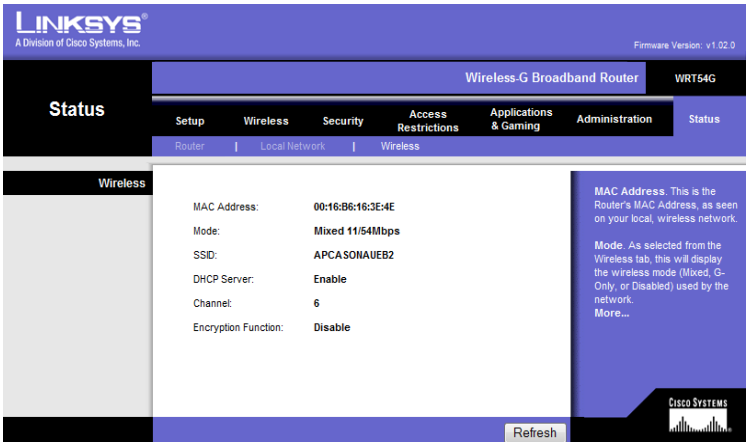


Fig. 2.119 Datos configurados del equipo

Fuente: Creación propia.

Dentro de Status se seleccionó Device List, donde podemos se observa todos los equipos conectados al Access Point.

DHCP Active IP Table

DHCP Server IP Address: **192.168.4.1** Refresh

Client Host Name	IP Address	MAC Address	Expires	Delete
MARCIA	192.168.1.121	00:24:2b:86:89:9b	23:58:05	☐
Principal	192.168.1.104	00:17:3f:d2:c8:6d	23:29:35	☐
MULTISYS	192.168.1.103	00:08:a1:a4:e4:80	17:50:26	☐
equipo1	192.168.1.120	00:1d:d9:07:2e:ea	12:15:43	☐
	192.168.1.119	00:21:fe:38:40:6d	09:13:00	☐
User	192.168.1.115	00:21:00:79:e5:73	06:12:22	☐
personal-c75f02	192.168.1.116	00:16:e3:71:47:fb	03:48:16	☐
user1	192.168.1.117	00:17:c4:25:42:29	03:37:32	☐

Close

Fig. 2.120 Ventana de usuarios conectados

Fuente: Creación propia.

Se ingresó al símbolo del sistema (MS-DOS) y se procedió a dar un ping a la dirección del router del Obispado 192.168.2.2 y a la dirección del router de la casona 192.168.2.1 verificando el tiempo de respuesta y el ancho de banda del enlace.

Se conectó inalámbricamente al Access point APCASONAUEB2 y se ingresó a internet verificando la tasa de transferencia.

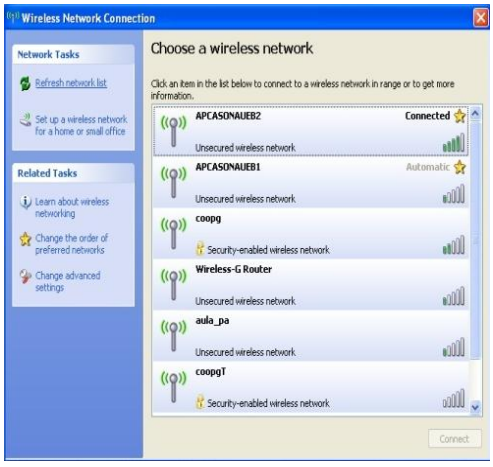


Fig. 2.121 Conectado al Access Point

Fuente: Creación propia

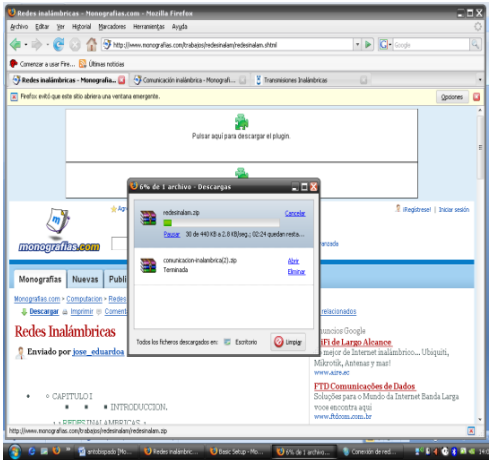


Fig. 2.122 Descarga de archivo

Fuente: Creación propia

El segundo punto instalado “Obispado”

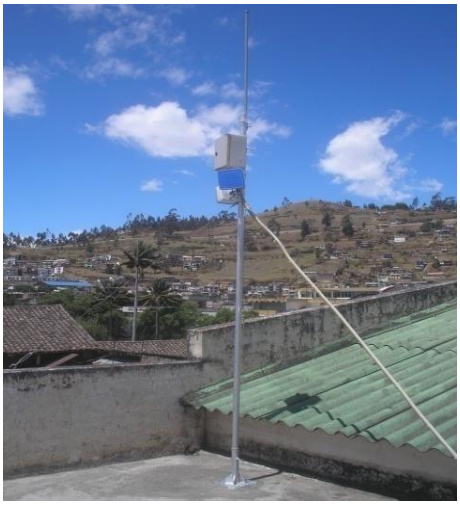


Fig. 2.123 Segundo punto Obispado

Fuente: Creación propia

3. Se instaló el tercer punto en La Casa Regional de Bolívar; un extremo del mástil de 3,20 m de longitud, se encajó en una bota metálica que se insertó en la visera y en el otro extremo se acondicionó el equipo, se sujetó la caja hermética al mástil con una abrazadera metálica en U, tornillos, arandelas de presión y tuercas.

Fig. 2.124 Acondicionamiento del Equipo

Fuente: Creación propia

La antena omnidireccional se sujetó en el extremo del mástil y sobre la caja hermética con abrazaderas metálicas en U, tornillos tuercas y arandelas de presión.

Fig. 2.125 Sujetación de la antena omnidireccional

Fuente: Creación propia

La antena direccional se la colocó en la parte inferior de la caja hermética sujetándola con abrazaderas galvanizadas.

Fig. 2.126 Sujetación de la antena direccional

Fuente: Creación propia

Se colocó una abrazadera para sujetar los tensores de alambre galvanizado los mismos que dieron firmeza al mástil. Se instaló una bota y una abrazadera metálica efectuando perforaciones en la pared de la visera de la Casa Regional de Bolívar con el taladro y la broca # 10, está última se la colocó a unos 50 cm de la bota metálica.

Se perforó la pared para introducir los cáncamos.

Fig. 2.127 Perforación de la visera
Fuente: Creación propia

Fig. 2.128 Colocación de la bota metálica
Fuente: Creación propia

Fig. 2.129 Perforación para la abrazadera metálica
Fuente: Creación propia

Fig. 2.130 Perforación de la pared
Fuente: Creación propia

Para equilibrar el mástil se utilizó los tensados y rompe vientos.

Fig. 2.131 Anclaje y tensado contra vientos
Fuente: Creación propia

Instalado el tercer punto se direccionó la antena directiva al segundo punto que se encuentra ubicado en el Obispado.

Fig. 2.132 Direccionando la antena hacia el obispado

Fuente: Creación propia

Instalado el tercer punto se revisó la caja hermética, abrazaderas, pernos y tuercas que estén bien ajustadas y se pintó con spray plateado las partes metálicas evitando la oxidación, esta revisión se realizó en los tres puntos.

Fig. 2.133 Revisión del equipo

Fuente: Creación propia

Fig. 2.134 Pintado de las partes metálicas

Fuente: Creación propia

Se enchufó el cable eléctrico y se conectó el cable de datos a la computadora portátil, se aguardó unos minutos hasta que el equipo esté listo, y se procedió a configurar el tercer punto:

Router Casa Regional de Bolívar (EECA)

Se seleccionó la pestaña Setup y se configuró: Automatic Configuration DHCP; Router Name: *EECAUEB*; Local IP Address: *192.168.2.3*; Subnet Mask: *255.255.255.0*; DHCP Server: *Disable*; Spanning Tree Protocol: *Disable*; Time Seting: *GMT-05-00 Indiana East, Colombia, Panama*; una vez realizados estos cambios se guardó *Save Settings*.

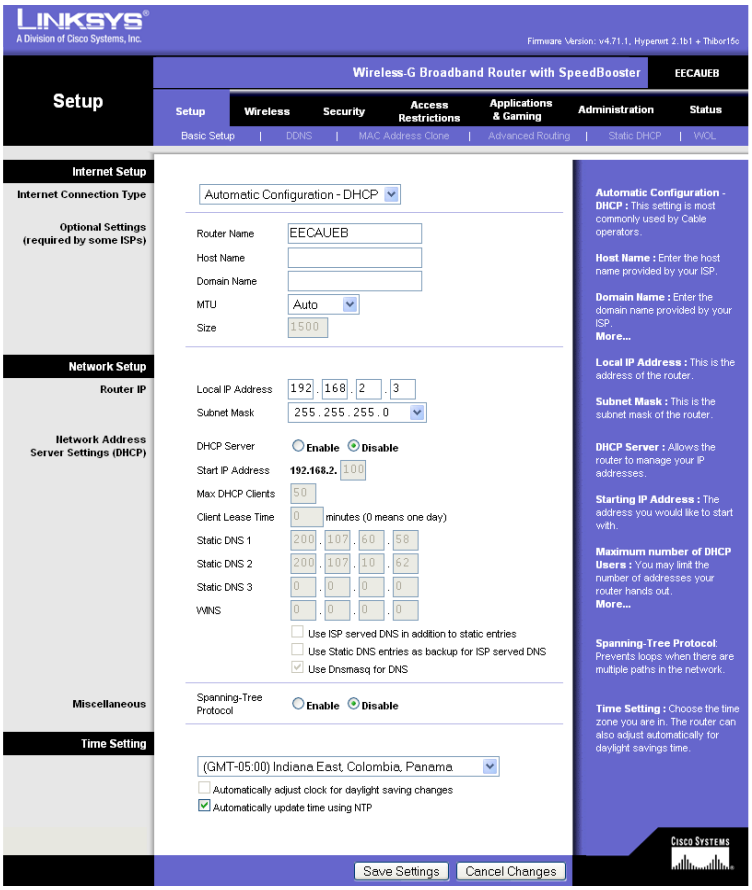


Fig. 2.135 Configuración del Setup

Fuente: Creación propia.

Se procesó los cambios, se activó la pestaña Wireless en la opción Basic Wireless Settings se seleccionó las siguientes opciones: Wireless Mode: *Access Point + WDS*; Wireless Netwok Mode: *Mixed*; Wireless Network Name (SSID): *EECAUEB*; Wireless Channel: *11-2.462 GHz*; Wireless SSID Broadcast: *Disable.*

En Mode: *Link with the following;* Remote Bridges:*00.21.29.D1.1E.FD*, es la dirección MAC del equipo que se enlaza (Repetidor), clic en *Save Settings.*

Fig. 2.136 Configuración de la pestaña Wireless

Fuente: Creación propia.

En Advanced Wireless Settings las trece primeras opciones se mantienen. Rx Antena: *Rigth*; Tx Antena: *Rigth*; Transmit Power: *Manual* y incrementó la potencia del radio a *150 mV*; se dio clic en *Save Settings* para guardar.

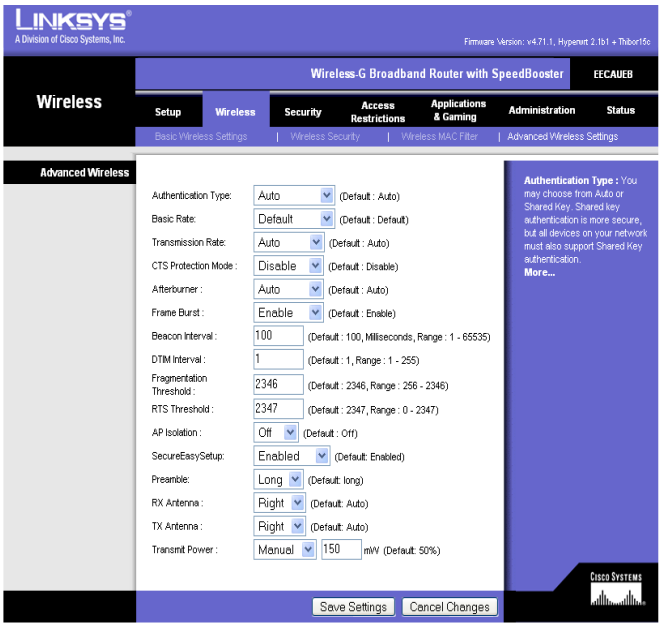


Fig. 2.137 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

Se espero unos segundos hasta que el equipo actualice los cambios.

En la pestaña Administración se seleccionó la opción Management se procedió a cambiar la contraseña (ruotereeca) con su respectiva confirmación; se activó las siguientes opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*, SSHD: *Disable;* Status Stopped: *Allow wireless Access;* se dio clic en *Save Settings* para guardar.

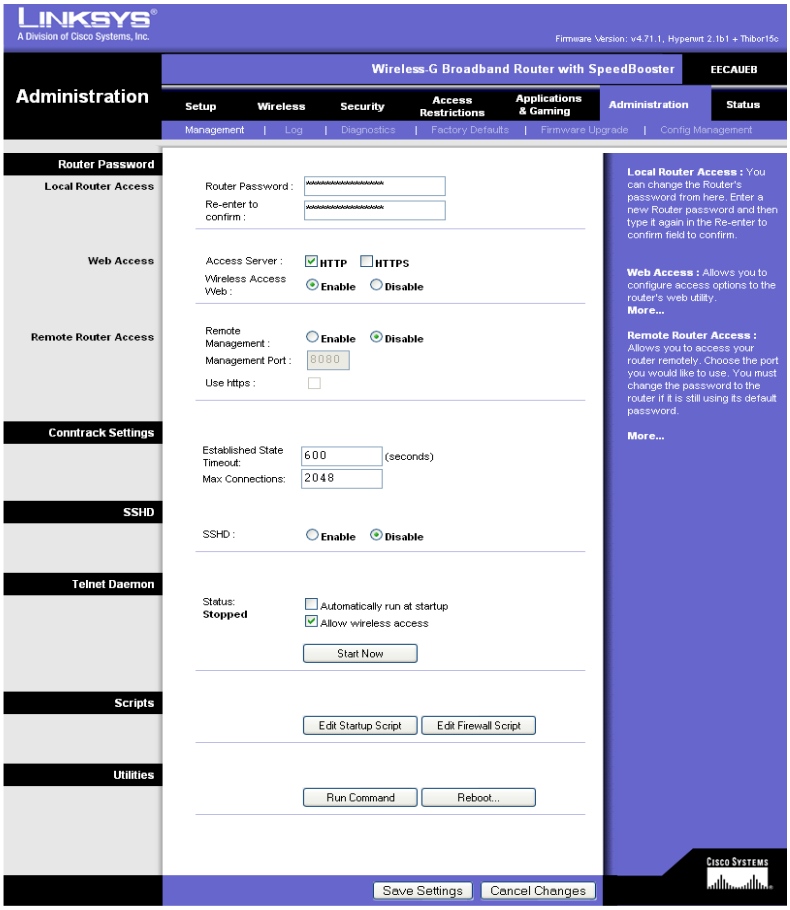


Fig. 2.138 Administración de contraseña de ingreso

Fuente: Creación propia.

En la pestaña Status en la opción Wireless, se observa las siguientes características: MAC Address: 00:1D:7E:F8:22:C4; Mode: Mixed; SSID: RepetidorUEB; DHCP Server: Disable; Chanel: 11; Encrytion Funtion: Disable.

Si se realiza alguna modificación dar clic en Refresh.

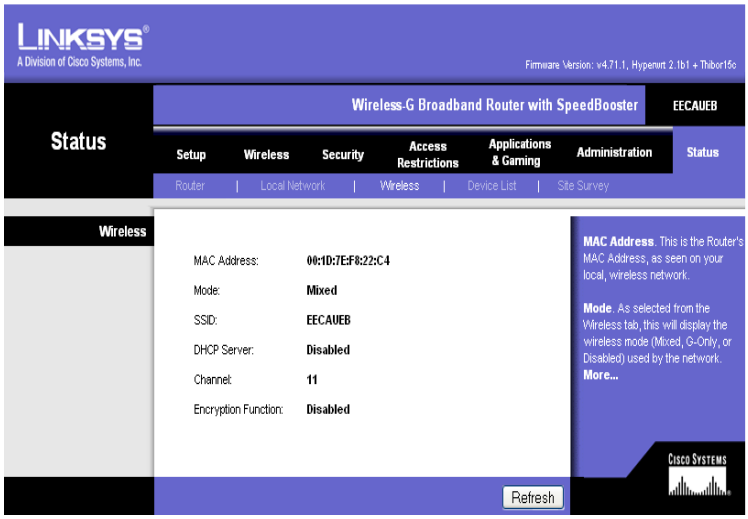


Fig. 2.139 Datos configurados del equipo

Fuente: Creación propia.

Se activó Site Survey, aquí se observa el SSIDS, el MAC Wireless, el canal de frecuencia y la potencia de los router inalámbricos que están operativos.

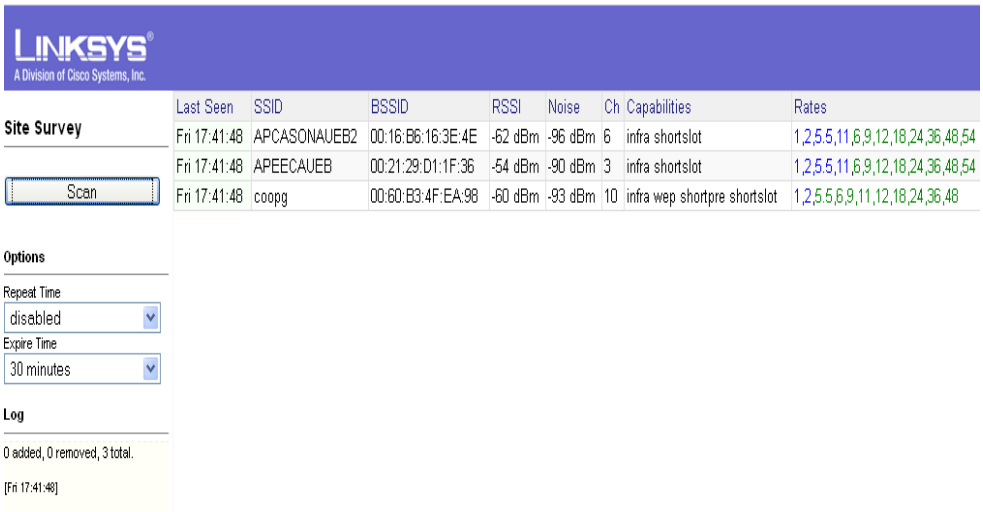


Fig. 2.140 Ventana de equipos operativos

Fuente: Creación propia.

Access Point Casa Regional de Bolívar (EECA)

Se ingresó a través de browser, se seleccionó la pestaña Setup y se configuró: Static IP con las siguientes direcciones; Internet IP Address: *192.168.2.13*; Subnet Mask: *255.255.255.0*; Gateway: *192.168.2.1*; Static

DNS 1: *200.107.60.58*; Static DNS 2: *200.107.10.62*; Router Name: *APEECAUEB.*

Local IP Address: *192.168.5.1*; Subnet Mask: *255.255.255.0*; DHCP Server:*Enable*; Start IP Address: *192.168.5.100*; Max DHCP Clients: *20*, se puede aumentar el número de clientes pero no es recomendable ya que disminuyeria el ancho de banda; Client Lease Time: *60* minutes; Activamos: Use Dnsmasq for DNS; Spanning Tree Protocol: *Disable;* una vez realizados estos cambios se guardo dando clic en *Save Settings*.

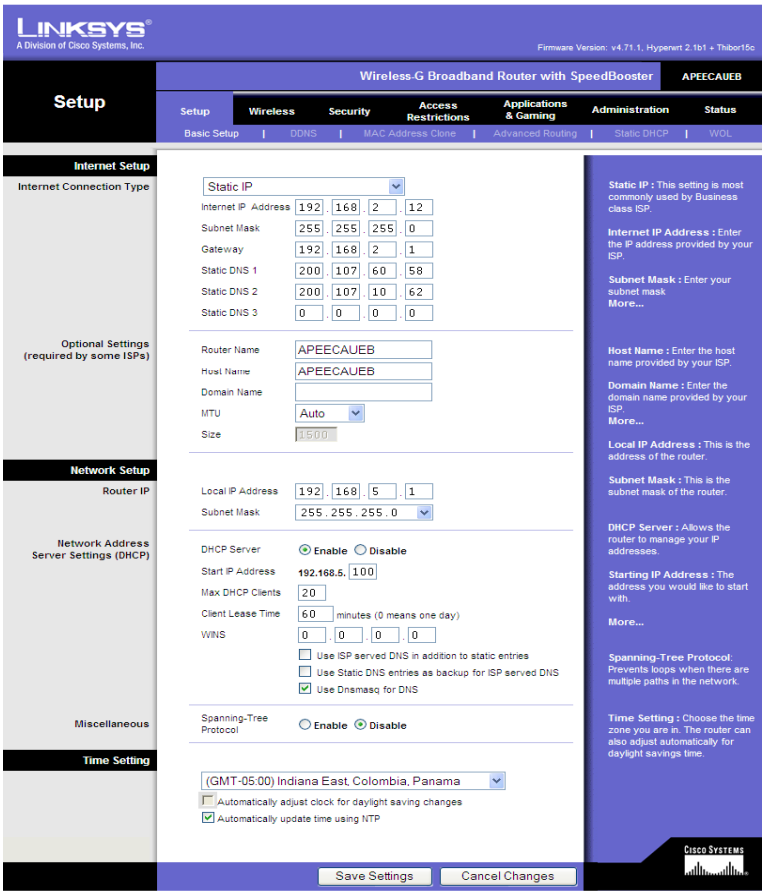


Fig. 2.141 Configuración del Setup

Fuente: Creación propia.

Se activó la pestaña Wireless, en Basic Wireless Settings se seleccionó las siguientes opciones: Wireless Mode: *Access Poin;* Wireless Netwok Mode: *Mixed*; Wireless Network Name(SSID):*APEECAUEB*; Wireless Channel: 3-

2.462 GHz; Wireless SSID Broadcast: *Enable*, se guardó dando clic en *Save Settings*.

Fig. 2.142 Configuración de la pestaña Wireless

Fuente: Creación propia.

Se seleccionó Advanced Wireless Settings las trece primeras opciones se mantienen. Rx Antena: *Right*; Tx Antena: *Right*, Transmit Power: *Manual* e incrementamos la potencia del radio a *100 mV*, se dió clic en *Save Settings*.

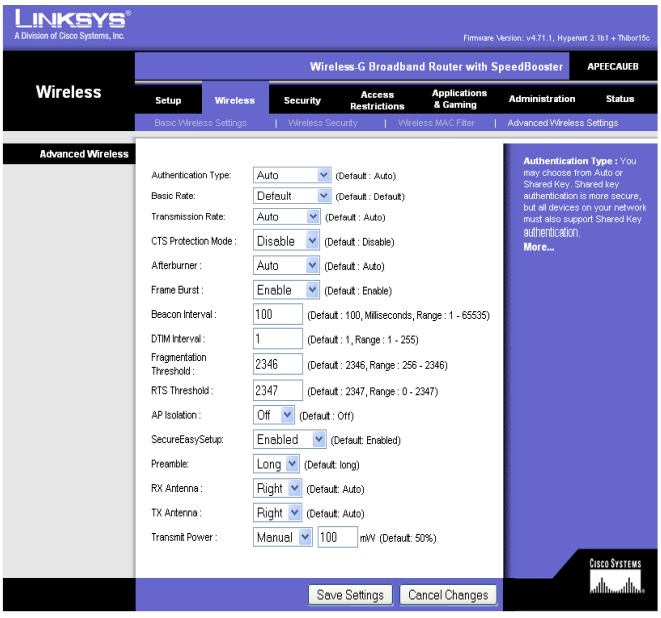


Fig. 2.143 Configuración de Advanced Wireless Settings

Fuente: Creación propia.

En la pestaña Administración se seleccionó la opción Management, se procedió a cambiar la contraseña (apeeca) con su respectiva confirmación; se activó las siguientes opciones; Access Server: *HTTP;* Wireless Access Web: *Enable;* Remote Management: *Disable*, Estabished state timeout; *600 (*seconds*);* Max Connections: *2048*; SSHD: *Disable;* Status Stopped: *Allow wireless Access;* se dio clic en *Save Settings* para guardar.

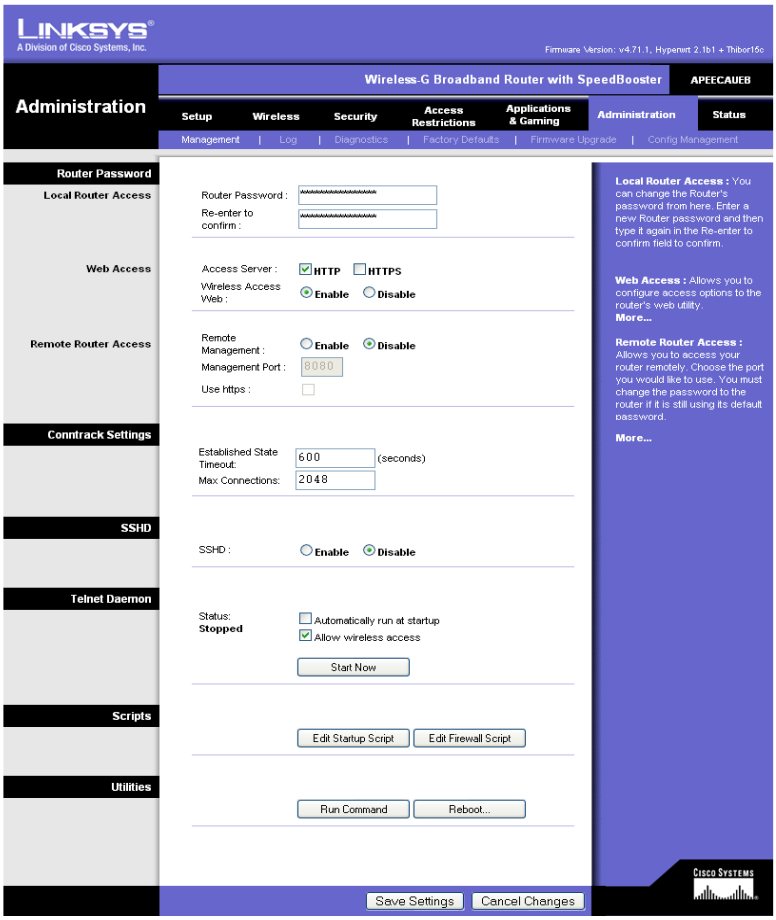


Fig. 2.144 Administración de constraseña de ingreso

Fuente: Creación propia

En Status en la opción Site Survey observamos los SSIDS, el MAC Address, el canal de frecuencias y la potencia que tienen los equipos que están instalados a su entorno.

Dentro de Status se seleccionó Device List, donde podemos se observa todos los equipos conectados al Access Point.

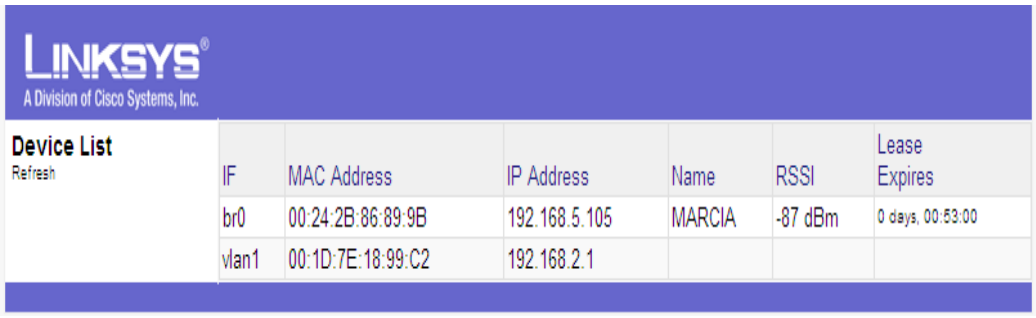


Fig. 2.145 Ventana de usuarios conectados

Fuente: Creación propia.

Se ingresó al símbolo del sistema (MS-DOS) y dio a dar un ping a la dirección del router de la Casa Regional de Bolívar 192.168.2.3, a la dirección del router del Obispado 192.168.2.2 y al router de La Casona Universitaria 192.168.2.1, verificando el tiempo de respuesta y el ancho de banda del enlace.

Se conectó inalámbricamente al Access point APEECAUEB y se ingresó a internet verificando la tasa de transferencia.

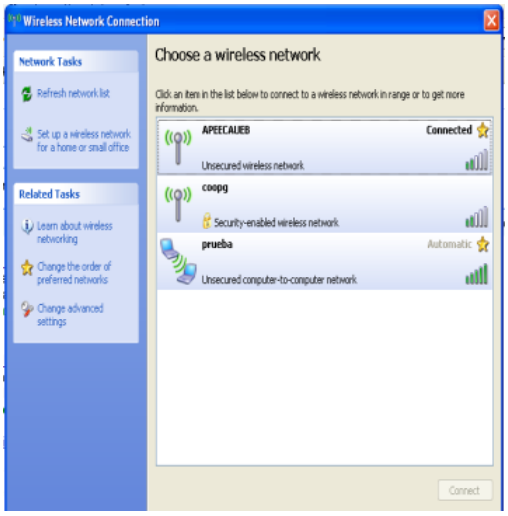


Fig. 2. 146 Conectado al Access Point

Fuente: Creación propia

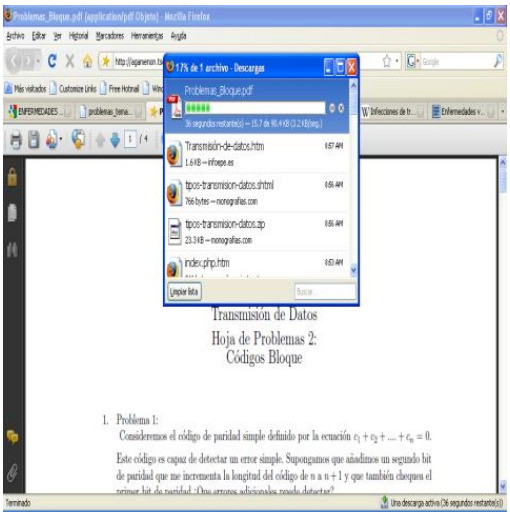


Fig. 2.147 Descargando un archivo

Fuente: Creación propia

El tercer punto instalado “Casa Regional de Bolívar (EECA)”

Fig. 2.148 Tercer punto Casa Regional de Bolívar

Fuente: Creación propia

Terminada la implementación de los tres puntos, se procedió a configurar las seguridades de ingreso a los Access Point.

Se activó la pestaña Wireless dentro del cual se seleccionó Wireless Security. En Security Mode se despliega varias opciones de las cuales se eligió WPA Personal.

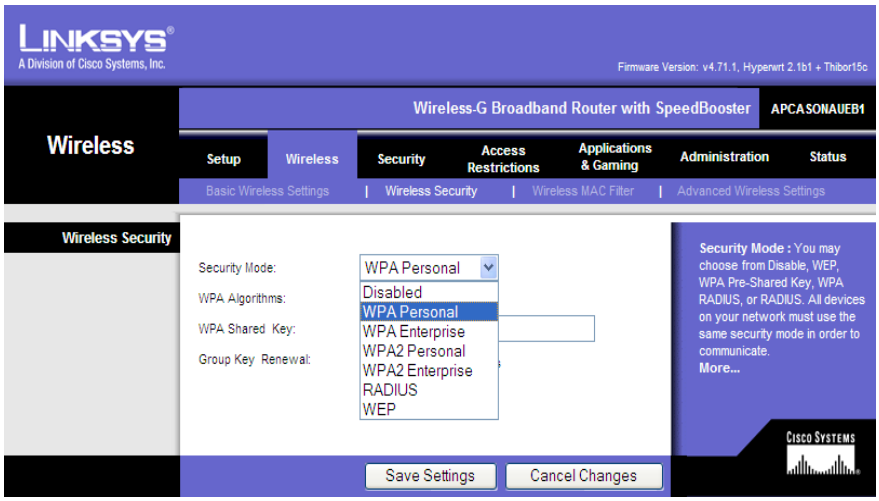


Fig. 2.149 Ventana de seguridades Wireless

Fuente: Creación propia

Se configuró el WPA Algorithms: TKIP; WPA Shared Key: apuebnetredes2009; Group Key Renewal: 3600 seconds.

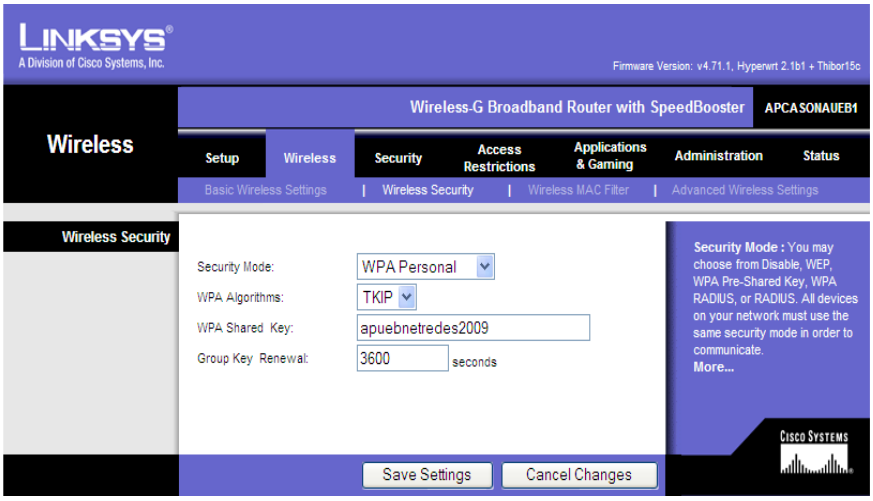


Fig. 2.150 Configuración de la seguridad wireless.

Fuente: Creación propia

La contraseña es apuebnetredes2009 para los tres Access Point encriptados que se muestran en la siguiente pantalla.

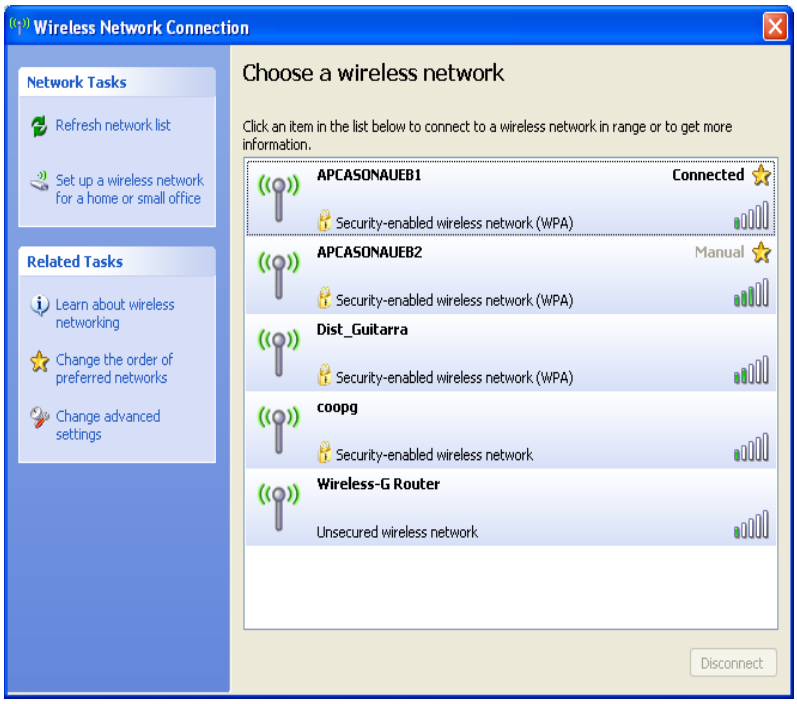


Fig. 2.151 Ventana de los Access Point encriptados

Fuente: Creación propia

2.5 MONITOREO DE LA TRANSMISIÓN DE DATOS DEL ENLACE POR RADIO

El monitoreo se realizó con las herramientas Iperf y Ping.

Iperf.- Para el proceso se corrió la aplicación Iperf en ambos extremos del enlace, se activó el iperf como servidor, y en el otro extremo del enlace como cliente (host).

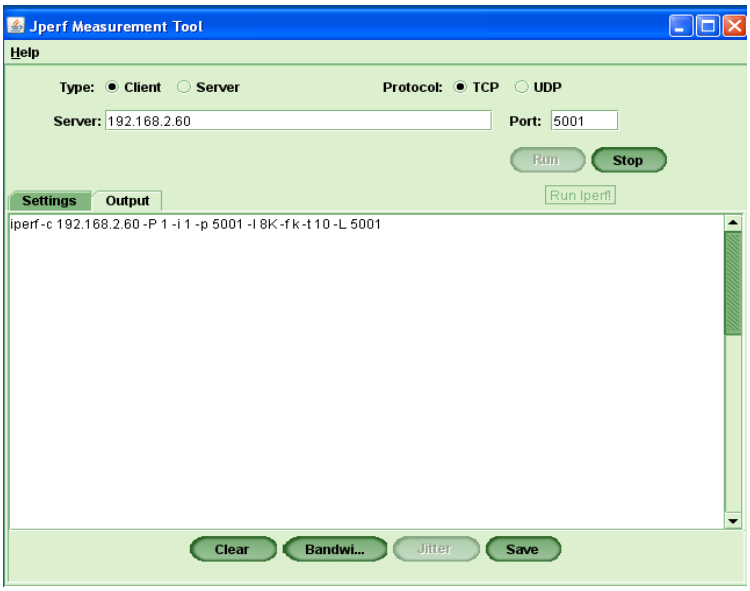


Fig. 2.152 Activado en modo cliente y establecida la conexión

Fuente: Creación propia

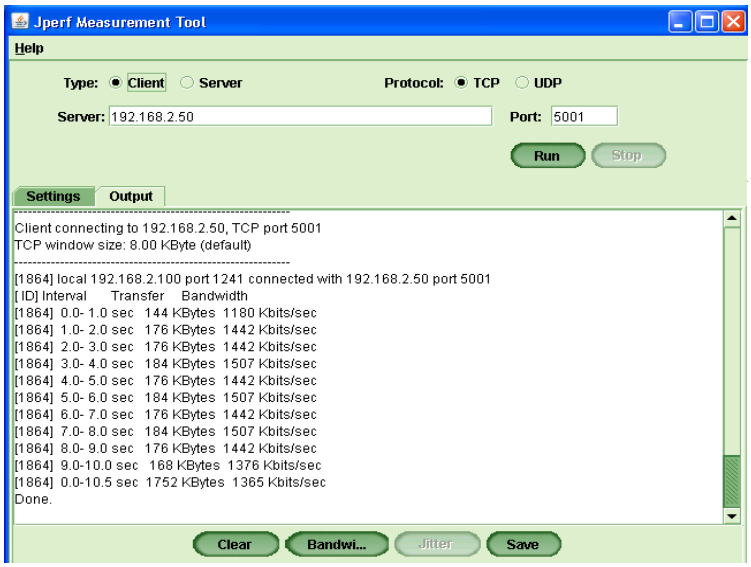


Fig. 2.153 Ejecutada y terminada la conexión

Fuente: Creación propia

Terminada la ejecución del iperf en modo cliente se desplegó el resultado del ancho de banda que se utilizó en la transmisión de los datos.

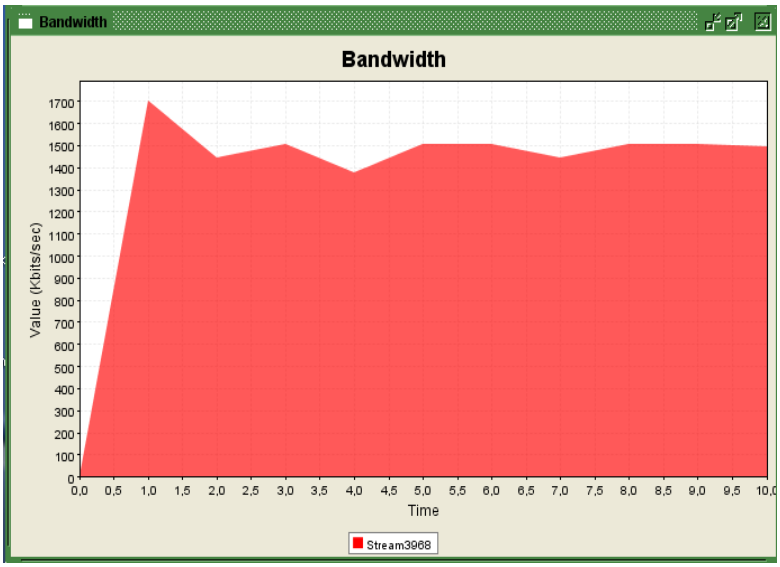


Fig. 2.154 Grafica del ancho de banda en función del tiempo

Fuente: Creación propia

Iperf activado en modo servidor

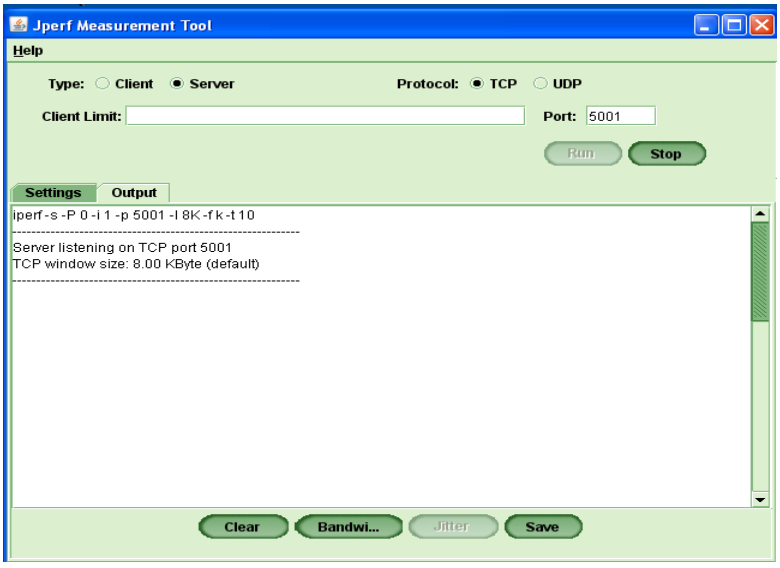


Fig.2.155 Establecida la conexión.

Fuente: Creación propia

Ejecución del iperf en modo servidor

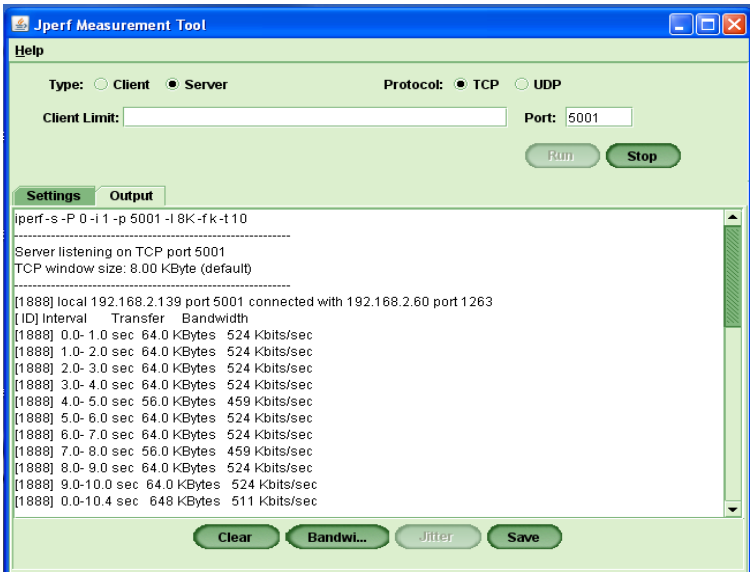


Fig. 2.156 Ejecutada y terminada la conexión

Fuente: Creación propia

Se desplegó el resultado del ancho de banda que se utilizó en la transmisión de los datos.

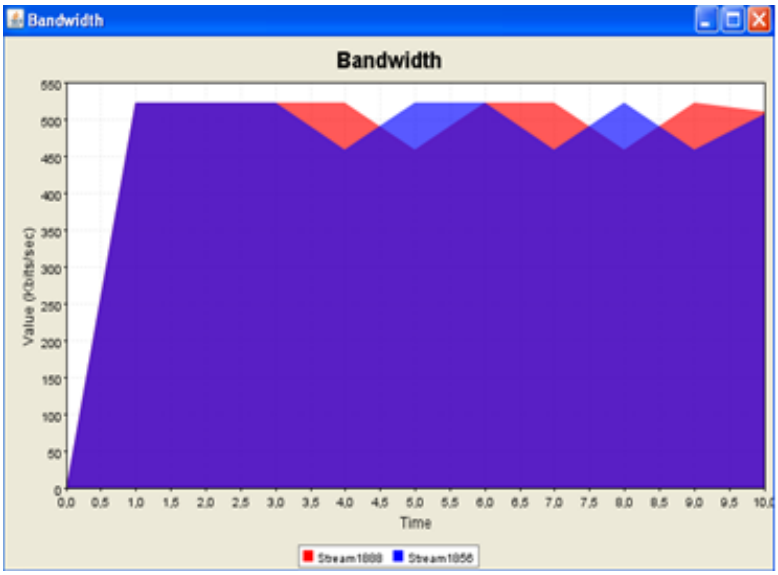


Fig. 2.157 Grafica del ancho de banda de varias conexiones en función del tiempo

Fuente: Creación propia

PING.- Se realizó un ping entre dos terminales (Casa Regional de Bolívar - Casona Universitaria) así se examinó si hay o no problemas en la red, y el tiempo de respuesta

en la trasmisión de datos. Ping desde una computadora de la Casona Universitaria 192.168.2.139 a una computadora de la Casa Regional de Bolívar 192.168.2.60

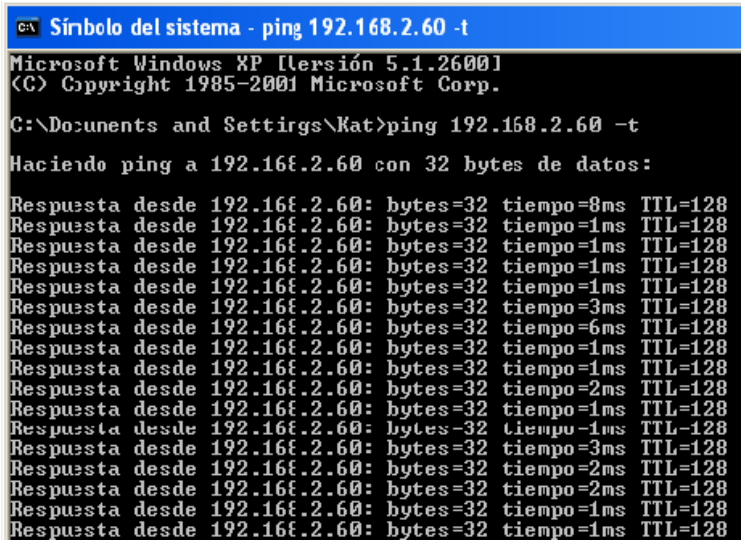


Fig. 2.158 Ping a la dirección 192.168.2.60

Fuente: Creación propia

Terminado la ejecución los resultados fueron: paquetes enviados 2643, paquetes recibidos 2634 y paquetes perdidos 9; lo que significa el 0.34% de paquetes perdidos.

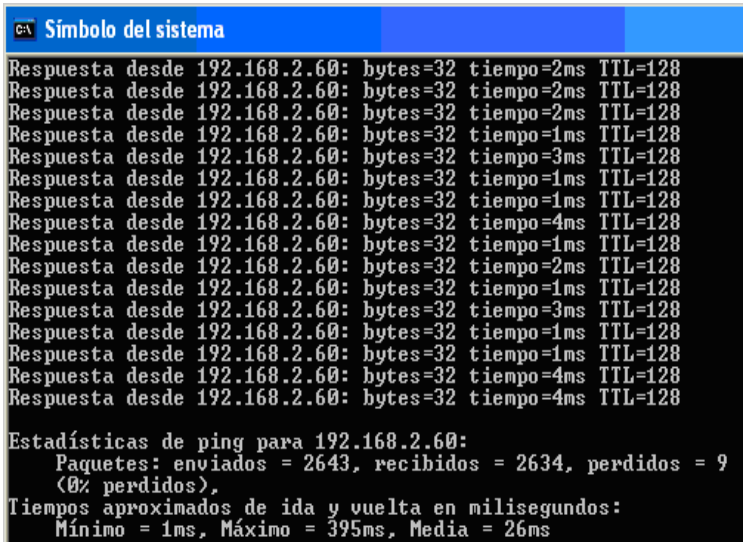


Fig. 2.159 Resultados obtenidos de la ejecución del ping

Fuente: Creación propia

Realizado el monitoreo del enlace por radio entre (Casona Universitaria - Casa Regional de Bolívar) se tabuló los datos por el lapso de cuatro meses: se realizó el promedio por

mes en modo cliente y en modo servidor, estimando el rendimiento del enlace con la herramienta Iperf, los datos se detallan a continuación:

MODO CLIENTE

MAYO

CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
04/05/09	1792	1784	8	1464	
06/05/09	1832	1824	8	1493	
08/05/09	1840	1832	8	1492	
12/05/09	1832	1824	8	1497	
13/05/09	1840	1832	8	1490	
14/05/09	1848	1840	8	1494	
18/05/09	1840	1832	8	1489	
20/05/09	1840	1832	8	1495	
22/05/09	1840	1832	8	1492	
26/05/09	1744	1736	8	1420	
28/05/09	1832	1824	8	1418	
29/05/09	1840	1832	8	1490	
PROMEDIO	**21920**		**96**	**17734**	**0.44**

Cuadro. 2.5 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

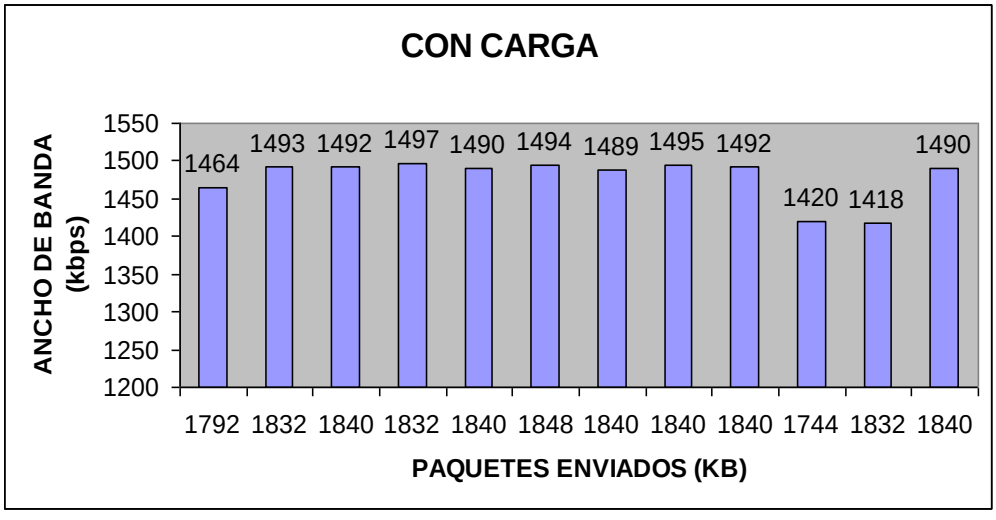


Fig. 2.160 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

Paquetes enviados en el mes de mayo sin carga en modo cliente

SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
04/05/09	624	616	8	499	
06/05/09	632	624	8	508	
08/05/09	632	624	8	509	
12/05/09	648	640	8	510	
13/05/09	632	624	8	505	
14/05/09	648	640	8	511	
18/05/09	632	624	8	482	
20/05/09	624	616	8	503	
22/05/09	632	624	8	507	
26/05/09	528	520	8	419	
28/05/09	632	624	8	507	
29/05/09	632	624	8	510	
PROMEDIO	**7496**		**96**	**5970**	**1.28**

Cuadro. 2.6 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

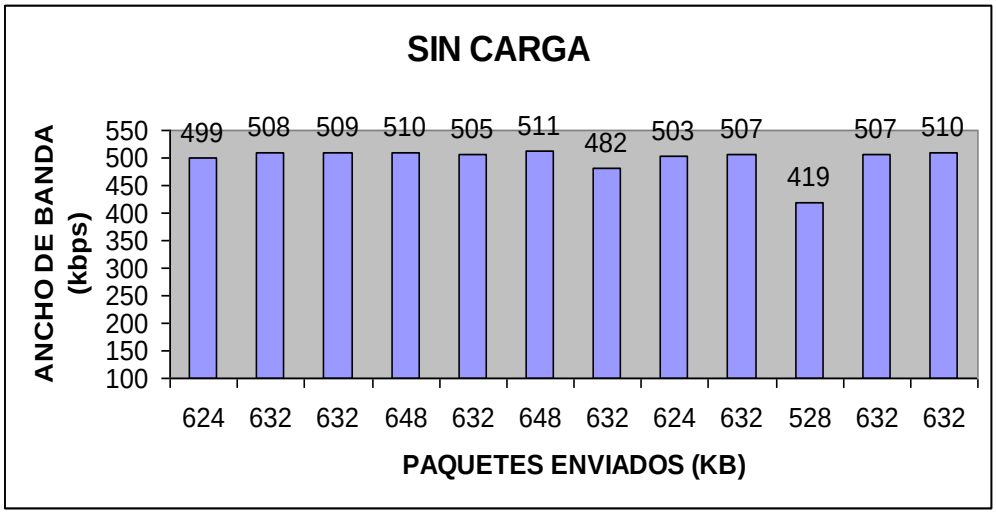


Fig. 2.161 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

JUNIO

CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/06/09	1848	1840	8	1494	
03/06/09	1848	1840	8	1495	
05/06/09	1840	1832	8	1498	
09/06/09	1840	1832	8	1495	
10/06/09	1848	1840	8	1494	
11/06/09	1840	1832	8	1492	
15/06/09	1814	1806	8	1484	
17/06/09	1840	1832	8	1487	
19/06/09	1840	1832	8	1495	
23/06/09	1816	1808	8	1480	
25/06/09	1840	1832	8	1493	
26/06/09	1848	1840	8	1497	
29/06/09	1848	1840	8	1497	
PROMEDIO	**23910**		**104**	**19401**	**0.43**

Cuadro 2.7 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

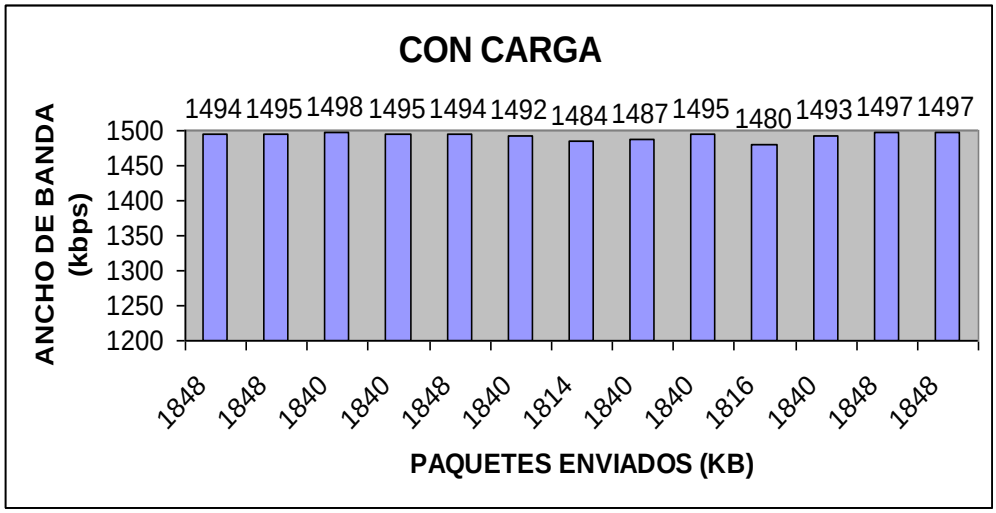


Fig. 2.162 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

Paquetes enviados en el mes de junio sin carga en modo cliente

SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/06/09	648	640	8	510	
03/06/09	576	568	8	463	
05/06/09	648	640	8	510	
09/06/09	632	624	8	509	
10/06/09	632	624	8	506	
11/06/09	576	568	8	459	
15/06/09	480	472	8	387	
17/06/09	584	576	8	469	
19/06/09	552	544	8	442	
23/06/09	456	448	8	365	
25/06/09	424	416	8	337	
26/06/09	536	528	8	419	
29/06/09	456	448	8	357	
PROMEDIO	**7200**		**104**	**5733**	**1.44**

Cuadro.2.8 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

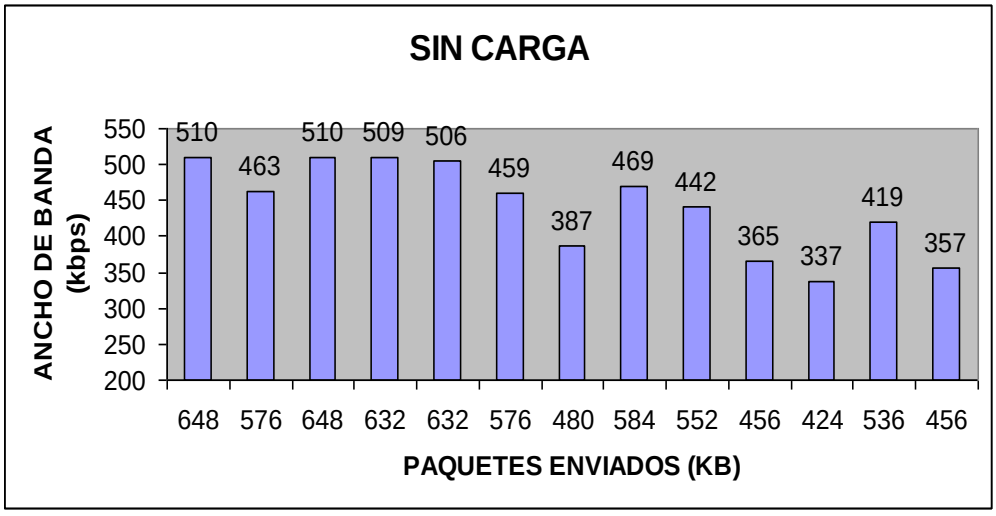


Fig. 2.163 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

JULIO

CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/07/09	1848	1840	8	1494	
03/07/09	1848	1840	8	1495	
07/07/09	1840	1832	8	1493	
08/07/09	1840	1832	8	1490	
09/07/09	1840	1832	8	1493	
13/07/09	1840	1832	8	1493	
15/07/09	1832	1824	8	1485	
17/07/09	1840	1832	8	1492	
21/07/09	1824	1816	8	1480	
23/07/09	1840	1832	8	1422	
24/07/09	1848	1840	8	1495	
27/07/09	1794	1786	8	1443	
29/07/09	1832	1824	8	1493	
31/07/09	1830	1822	8	1413	
PROMEDIO	**25696**		**112**	**20681**	**0.44**

Cuadro. 2.9 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

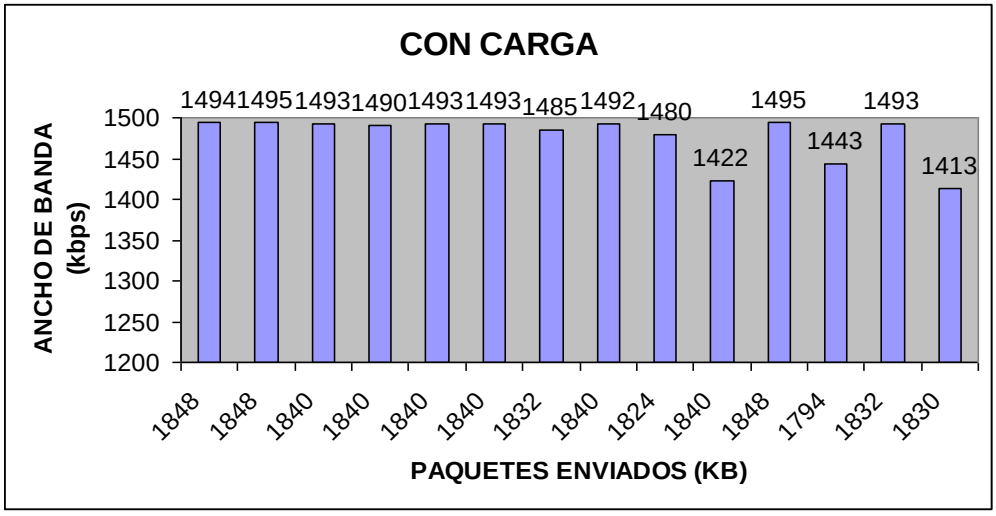


Fig. 2. 164 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

Paquetes enviados en el mes de julio sin carga en modo cliente

SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/07/09	488	480	8	472	
03/07/09	448	440	8	432	
07/07/09	464	456	8	417	
08/07/09	512	504	8	404	
09/07/09	504	496	8	405	
13/07/09	472	464	8	403	
15/07/09	552	544	8	429	
17/07/09	512	504	8	411	
21/07/09	528	520	8	414	
23/07/09	536	528	8	418	
24/07/09	632	624	8	508	
27/07/09	448	440	8	410	
29/07/09	632	624	8	506	
31/07/09	632	624	8	509	
PROMEDIO	**7360**		**112**	**6138**	**1.52**

Cuadro.2.10 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

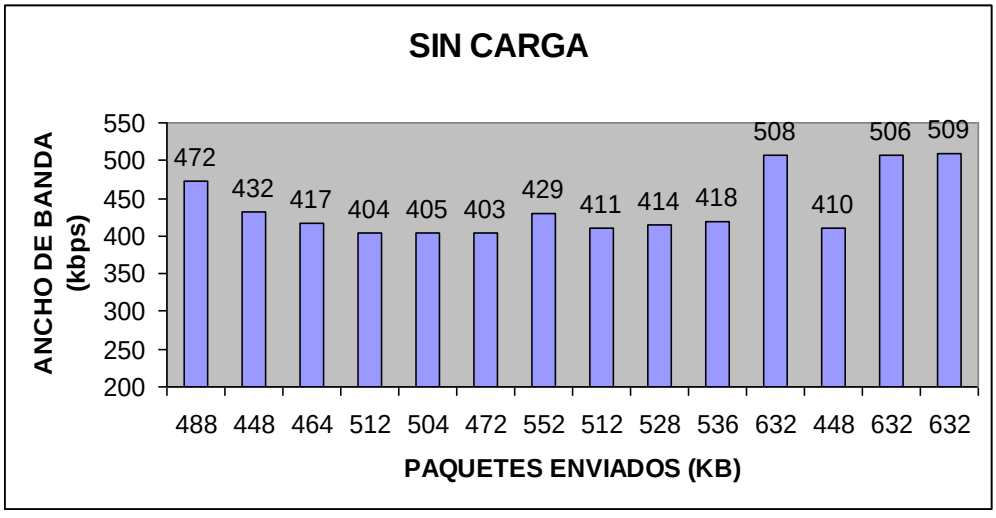


Fig. 2. 165 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

AGOSTO

CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
03/08/09	1840	1832	8	1487	
05/08/09	1848	1840	8	1498	
07/08/09	1832	1824	8	1493	
11/08/09	1688	1680	8	1367	
12/08/09	1688	1680	8	1366	
13/08/09	1680	1672	8	1366	
17/08/09	1568	1560	8	1305	
19/08/09	1618	1610	8	1328	
21/08/09	1848	1840	8	1497	
25/08/09	1752	1744	8	1334	
27/08/09	1832	1824	8	1491	
28/08/10	1680	1672	8	1355	
31/08/11	1840	1832	8	1496	
PROMEDIO	**22714**		**104**	**18383**	**0.46**

Cuadro.2.11 Paquetes enviados en modo cliente con carga

Fuente: Creación propia

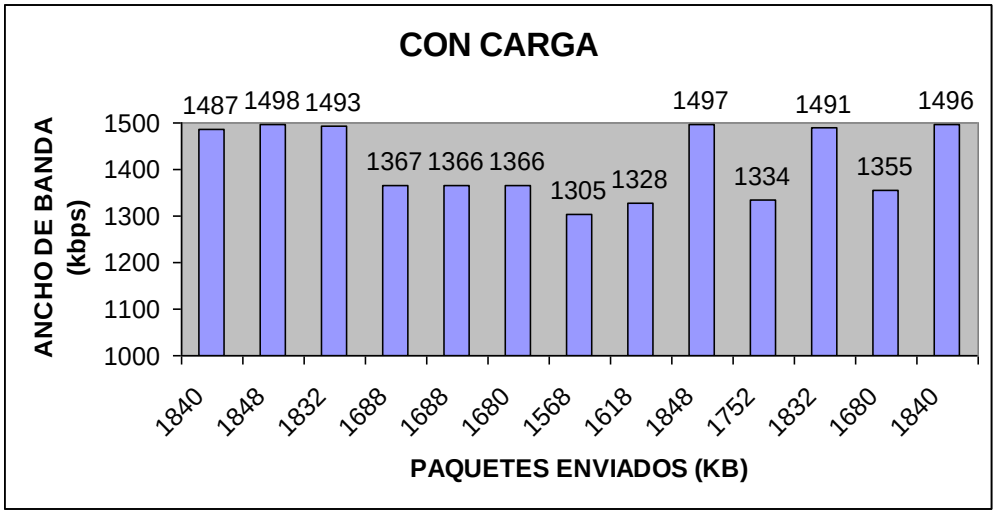


Fig. 2. 166 Paquetes enviados en modo cliente con carga

Fuente: Creación Propia

Paquetes enviados en el mes de agosto sin carga en modo cliente

SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
03/08/09	624	616	8	504	
05/08/09	648	640	8	510	
07/08/09	616	608	8	500	
11/08/09	628	620	8	507	
12/08/09	624	616	8	502	
13/08/09	640	632	8	505	
17/08/09	640	632	8	506	
19/08/09	648	640	8	510	
21/08/09	648	640	8	510	
25/08/09	600	592	8	500	
27/08/09	624	616	8	504	
28/08/10	632	624	8	509	
31/08/11	624	616	8	504	
PROMEDIO	**8196**		**104**	**6571**	**1.27**

Cuadro. 2.12 Paquetes enviados en modo cliente sin carga

Fuente: Creación propia

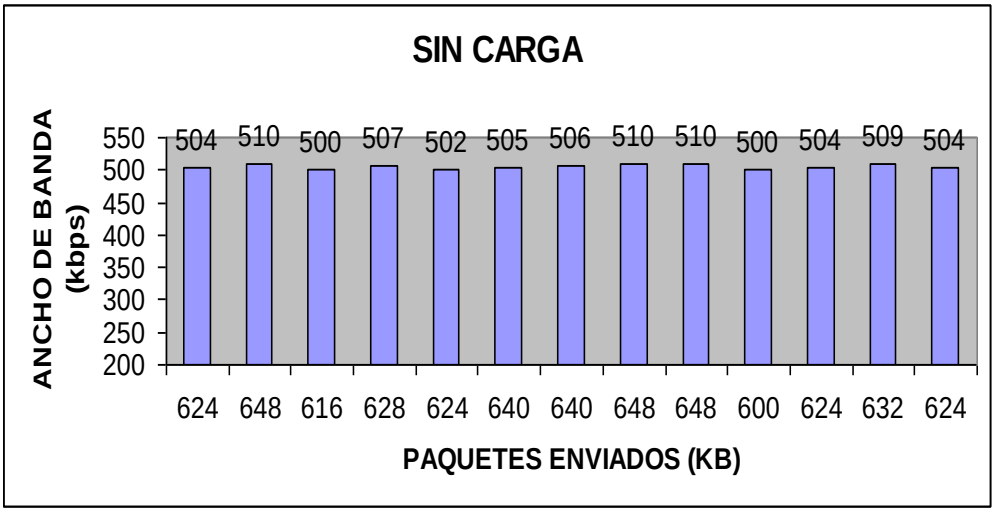


Fig. 2.167 Paquetes enviados en modo cliente sin carga

Fuente: Creación Propia

Promedios Clientes

Datos en modo cliente con carga:

En el mes de julio se evidencia un incremento del promedio 25696 paquetes enviados con un ancho de banda de 20681, siendo el mes en el que se transmitió el mayor número de paquetes.

CON CARGA		
FECHA	**PAQUETES ENVIADOS (KB)**	**ANCHO DE BANDA (Kbps)**
MAYO	21920	17734
JUNIO	23910	19401
JULIO	25696	20681
AGOSTO	22714	18383

Cuadro. 2.13 Promedio de paquetes enviados por meses

Fuente: Creación propia

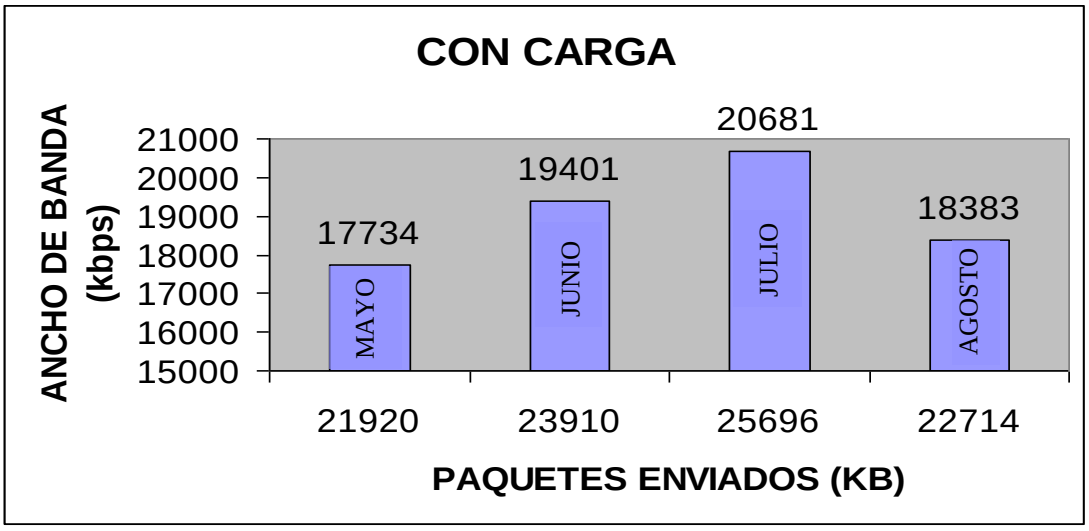


Fig. 2.168 Promedio de paquetes enviados en modo cliente con carga

Fuente: Creación propia

Datos en modo cliente sin carga:

En el mes de Agosto se evidencio un incremento del promedio 8196 paquetes enviados con un ancho de banda de 6571 siendo el mes en el cual se transmitió el mayor número de paquetes.

SIN CARGA		
FECHA	**PAQUETES ENVIADOS (KB)**	**ANCHO DE BANDA (Kbps)**
MAYO	7496	5970
JUNIO	7200	5733
JULIO	7360	6138
AGOSTO	8196	6571

Cuadro. 2.14 Promedio de paquetes enviados por meses

Fuente: Creación propia

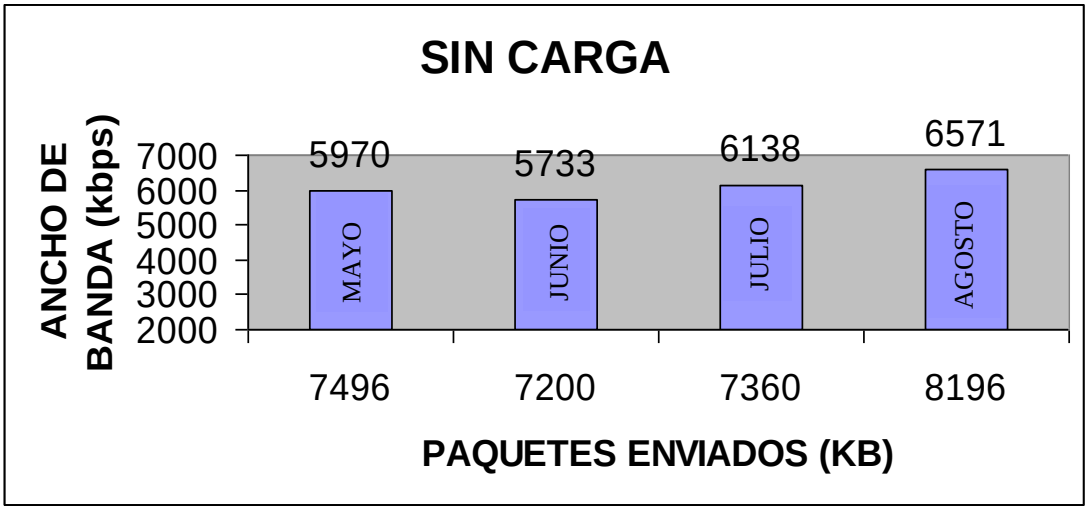


Fig. 2.169 Promedio de paquetes enviados en modo cliente sin carga

Fuente: Creación propia

MODO SERVIDOR

MAYO

SERVIDOR CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
04/05/09	1832	1808	24	1534	
06/05/09	1746	1730	16	1502	
08/05/09	1840	1816	24	1491	
12/05/09	1832	1816	16	1487	
13/05/09	1824	1808	16	1483	
14/05/09	1744	1728	16	1486	
18/05/09	1832	1816	16	1489	
20/05/09	1752	1728	24	1486	
22/05/09	1832	1800	32	1480	
26/05/09	1832	1816	16	1487	
28/05/09	1810	1794	16	1479	
29/05/09	1806	1798	8	1485	
PROMEDIO	**21682**		**224**		**1.03**

Cuadro. 2.15 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

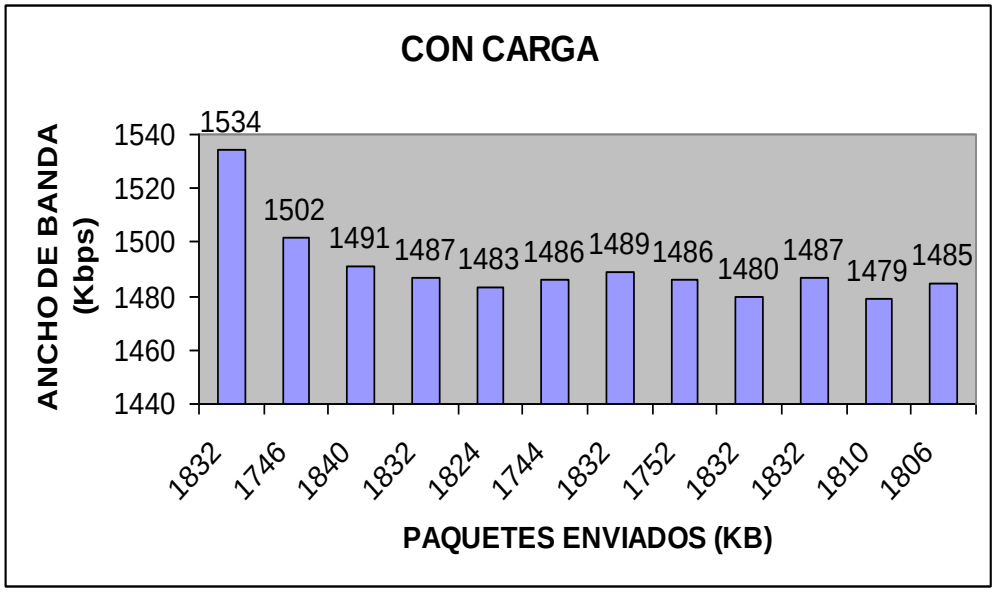


Fig. 2.170 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

Paquetes enviados en el mes de agosto con carga en modo servidor

SERVIDOR SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
04/05/09	632	616	16	505	
06/05/09	632	616	16	507	
08/05/09	576	560	16	461	
12/05/09	472	464	8	415	
13/05/09	464	448	16	423	
14/05/09	648	624	24	511	
18/05/09	624	608	16	500	
20/05/09	632	616	16	508	
22/05/09	648	624	24	511	
26/05/09	632	616	16	506	
28/05/09	616	600	16	501	
29/05/09	632	616	16	508	
PROMEDIO	**7208**		**200**	**5856**	**2.77**

Cuadro. 2.16 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

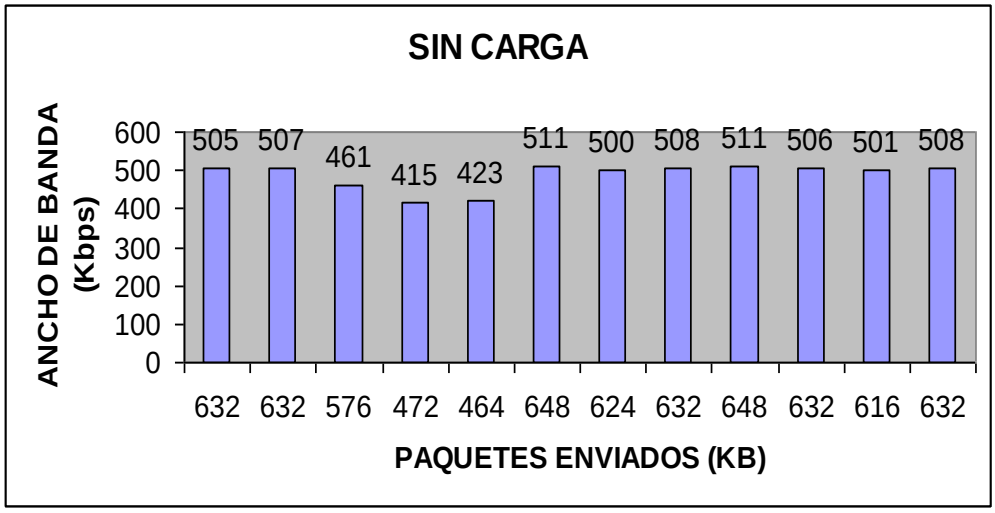


Fig. 2.171 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

JUNIO

SERVIDOR CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/06/09	1848	1832	16	1485	
03/06/09	1826	1802	24	1487	
05/06/09	1840	1816	24	1491	
09/06/09	1848	1824	24	1493	
10/06/09	1848	1816	32	1488	
11/06/09	1848	1824	24	1495	
15/06/09	1840	1816	24	1491	
17/06/09	1840	1808	32	1488	
19/06/09	1848	1816	32	1491	
23/06/09	1848	1816	32	1493	
25/06/09	1840	1816	24	1491	
26/06/09	1840	1824	16	1493	
29/06/09	1848	1816	32	1491	
PROMEDIO	**23962**		**336**		**1.40**

Cuadro. 2.17 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

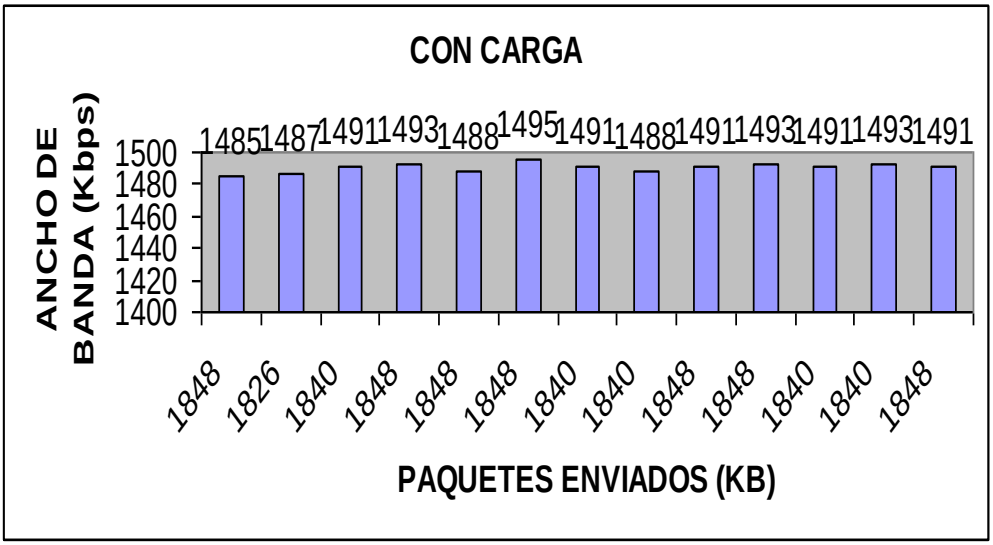


Fig. 2.172 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

Paquetes enviados en el mes de junio sin carga en modo servidor.

SERVIDOR SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/06/09	648	624	24	511	
03/06/09	640	616	24	510	
05/06/09	632	616	16	498	
09/06/09	632	616	16	507	
10/06/09	599	591	8	500	
11/06/09	624	608	16	501	
15/06/09	640	624	16	511	
17/06/09	601	585	16	501	
19/06/09	632	616	16	508	
23/06/09	648	624	24	512	
25/06/09	632	616	16	509	
26/06/09	648	624	24	512	
29/06/09	632	616	16	501	
PROMEDIO	**8208**		**232**	**6581**	**2.83**

Cuadro. 2.18 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

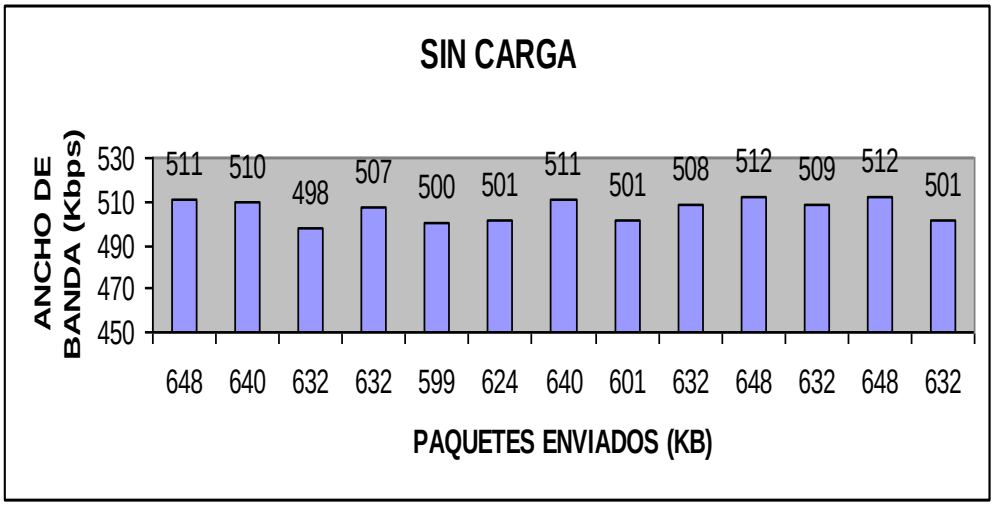


Fig. 2.173 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

JULIO

SERVIDOR CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/07/09	1840	1808	32	1486	
03/07/09	1720	1632	88	1486	
07/07/09	1840	1816	24	1486	
08/07/09	1840	1824	16	1493	
09/07/09	1816	1808	8	1478	
13/07/09	1840	1816	24	1491	
15/07/09	1848	1824	24	1493	
17/07/09	1832	1808	24	1482	
21/07/09	1840	1816	24	1489	
23/07/09	1824	1800	24	1476	
24/07/09	1840	1816	24	1491	
27/07/09	1803	1787	16	1475	
29/07/09	1744	1728	16	1467	
31/07/09	1704	1624	80	1455	
PROMEDIO	**25331**		**424**		**1.67**

Cuadro. 2.19 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

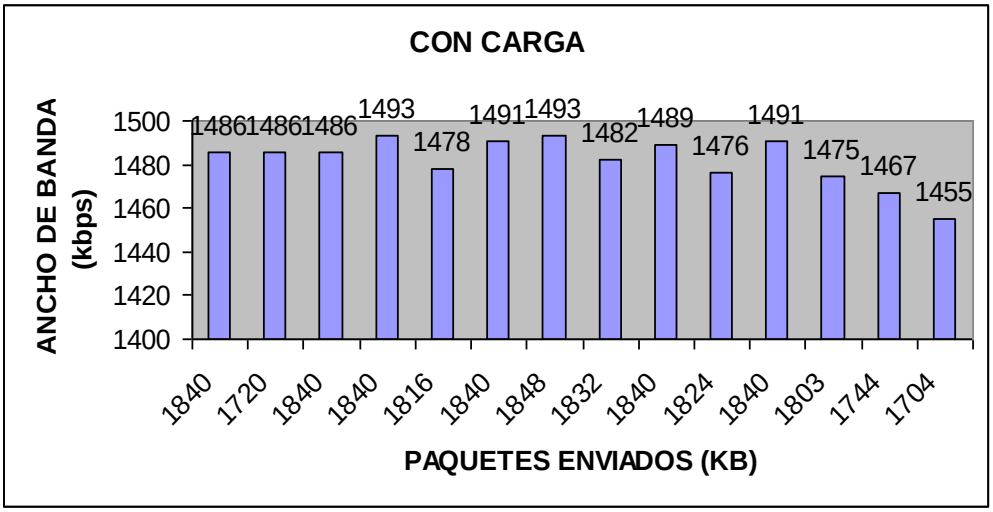


Fig. 2.174 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

Paquetes enviados en el mes de julio sin carga en modo servidor.

SERVIDOR SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
01/07/09	576	560	16	461	
03/07/09	480	464	16	384	
07/07/09	632	616	16	505	
08/07/09	624	616	8	505	
09/07/09	632	616	16	508	
13/07/09	528	503.93	24.07	420	
15/07/09	632	616	16	506	
17/07/09	632	616	16	510	
21/07/09	648	624	24	511	
23/07/09	576	560	16	463	
24/07/09	648	624	24	511	
27/07/09	632	616	16	510	
29/07/09	648	624	24	512	
31/07/09	376	360.2	15.8	303	
PROMEDIO	**8264**		**247.87**	**6609**	**3.00**

Cuadro. 2.20 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

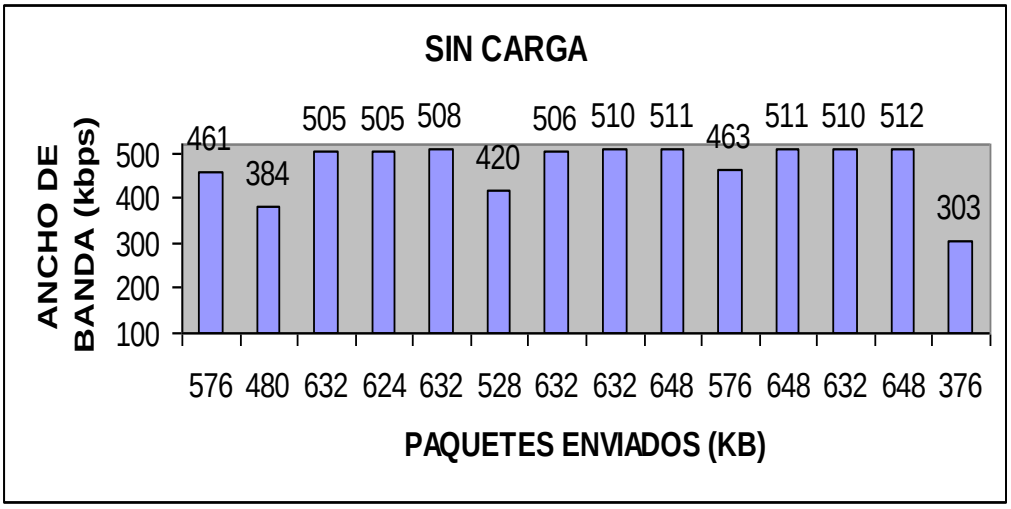


Fig. 2.175 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

AGOSTO

SERVIDOR CON CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
03/08/09	1752	1728	24	1329	
05/08/09	1840	1824	16	1486	
07/08/09	1848	1816	32	1491	
11/08/09	1744	1728	16	1418	
12/08/09	1848	1816	32	1491	
13/08/09	1848	1816	32	1491	
17/08/09	1848	1824	24	1495	
19/08/09	1824	1808	16	1483	
21/08/09	1752	1736	16	1422	
25/08/09	1488	1480.28	7.72	1210	
27/08/09	1728	1711.6	16.4	1402	
28/08/10	1744	1728	16	1418	
31/08/11	1728	1712	16	1402	
PROMEDIO	**22992**		**264.12**		**1.15**

Cuadro. 2.21. Paquetes enviados en modo servidor con carga

Fuente: Creación propia

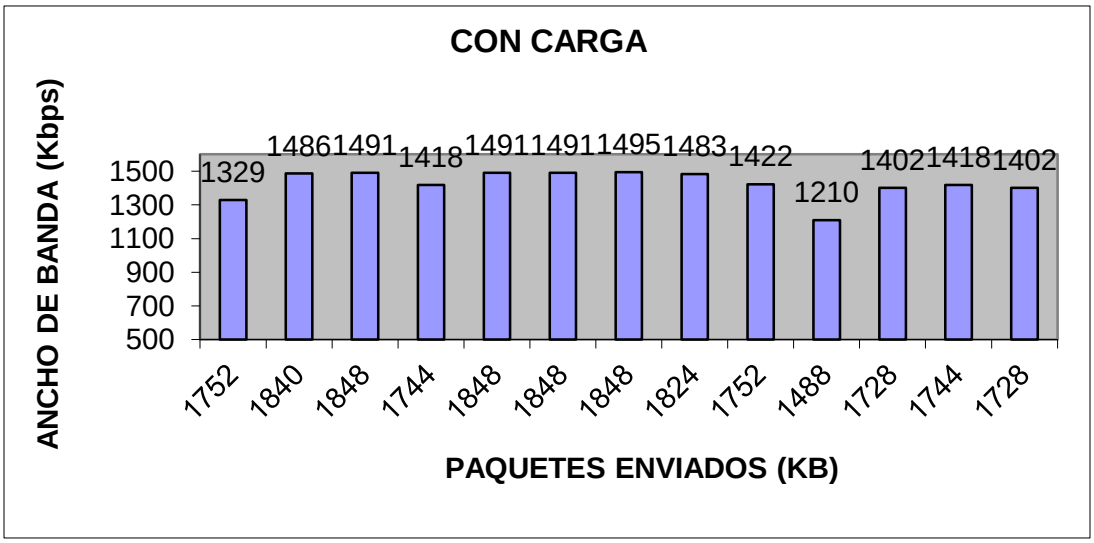


Fig. 2.176 Paquetes enviados en modo servidor con carga

Fuente: Creación propia

Paquetes enviados en el mes de agosto sin carga en modo servidor

SERVIDOR SIN CARGA					
FECHA	**PAQUETES ENVIADOS (KB)**	**PROMEDIO DE PAQUETES (KB)**	**PAQUETES PERDIDOS (KB)**	**ANCHO DE BANDA (Kbps)**	**%**
03/08/09	464	448	16	371	
05/08/09	480	472	8	384	
07/08/09	480	472	8	384	
11/08/09	576	552	24	463	
12/08/09	592	584	8	478	
13/08/09	464	448	16	371	
17/08/09	616	592	24	501	
19/08/09	528	504	24	420	
21/08/09	560	544	16	450	
25/08/09	648	624	24	511	
27/08/09	632	616	16	509	
28/08/10	640	616	24	510	
31/08/11	592	576	16	478	
PROMEDIO	**7272**		**224**	**5830**	**3.08**

Cuadro. 2.22 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

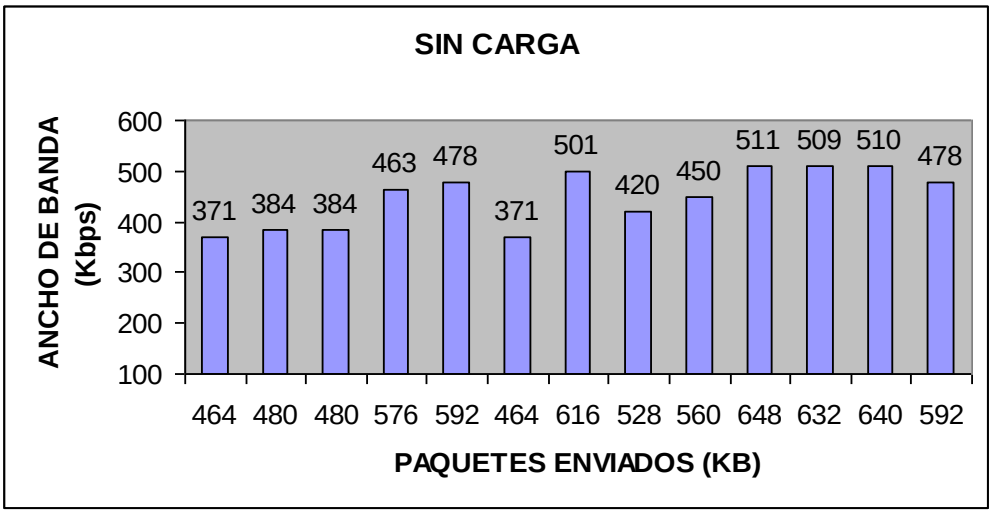


Fig. 2.177 Paquetes enviados en modo servidor sin carga

Fuente: Creación propia

Promedios en modo servidor

Datos en modo servidor con carga:

En el mes de Julio se evidencio un incremento del promedio 25331 paquetes enviados con un ancho de banda de 20748 siendo el mes en él se transmitió el mayor número de paquetes.

CON CARGA		
FECHA	**PAQUETES ENVIADOS (KB)**	**ANCHO DE BANDA (Kbps)**
MAYO	21682	17889
JUNIO	23962	19377
JULIO	25331	20748
AGOSTO	22992	18538

Cuadro. 2.23 Promedio de paquetes enviados por meses

Fuente: Creación propia

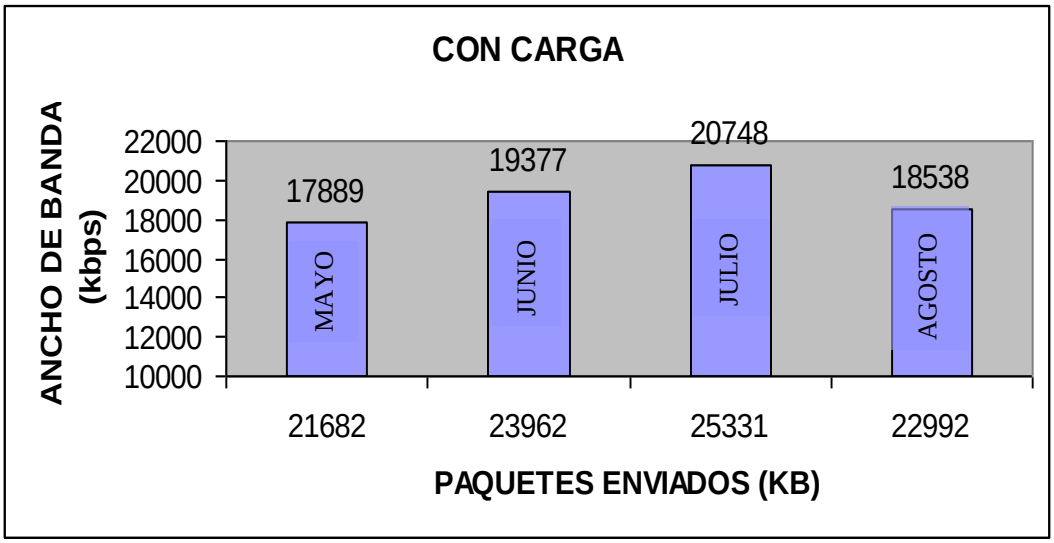


Fig. 2.178 Promedio de paquetes enviados en modo servidor con carga

Fuente: Creación propia

Datos en modo servidor sin carga:

En el mes de julio se evidencio un incremento del promedio 8264 paquetes enviados con un ancho de banda de 6609 siendo el mes en el que se transmitió el mayor número de paquetes enviados.

SIN CARGA		
FECHA	**PAQUETES ENVIADOS (KB)**	**ANCHO DE BANDA (Kbps)**
MAYO	7208	5856
JUNIO	8208	6581
JULIO	8264	6609
AGOSTO	7272	5830

Cuadro. 2.24 Promedio de paquetes enviados por meses

Fuente: Creación propia

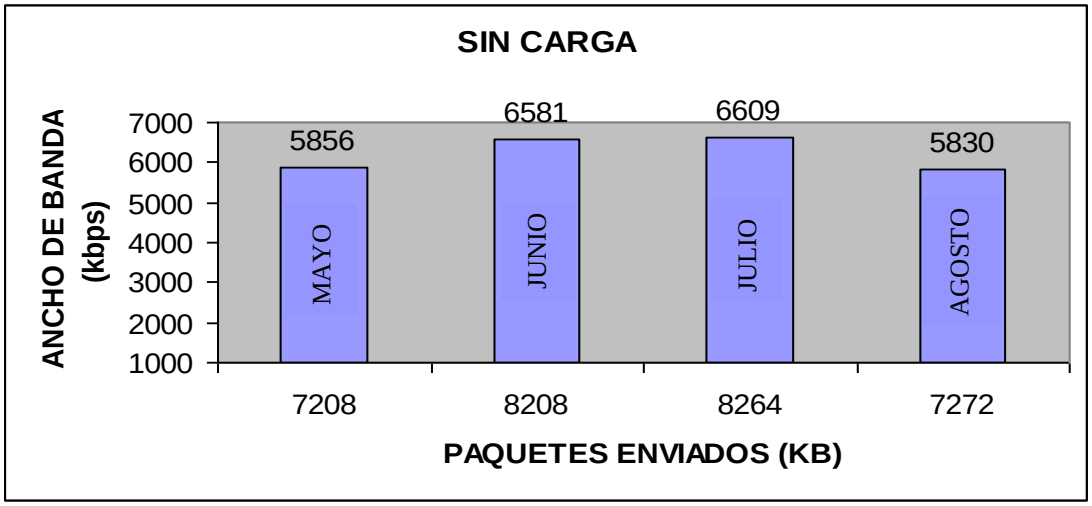


Fig.2.179 Promedio de paquetes enviados en modo servidor sin carga

Fuente: Creación propia

2.6 EVALUACIÓN DE LA TRANSMISIÓN DE DATOS DEL ENLACE

Concluidas las pruebas de monitoreo del enlace por radio entre la Casona Universitaria y la Casa Regional de Bolívar, se ha comprobado que este se encuentra en optimas condiciones. Quedando conectado el enlace a un switch marca C-Net de ocho puertos en la Casa Regional de Bolívar, donde se podría conectar una red interna; de esta manera

los departamentos de la Universidad que laboran en la Casa Regional de Bolívar están listos para integrarse a la red de datos de la Universidad Estatal de Bolívar.

Fig. 2.180 Switch habilitado en la Casa Regional de Bolívar

Fuente: Creación propia

Fig. 2.181 Conexión a internet en la Casa Regional de Bolívar

Fuente: Creación propia

Los tres puntos de Hot -Spot quedan operativos para el servicio de internet inalámbrico a la comunidad Universitaria.

CONCLUSIONES

- El hardware y el software utilizados para la implementación permiten un correcto funcionamiento del radio enlace.

- El diseño realizado si permitió la correcta identificación de los puntos estratégicos para la instalación de los equipos del enlace entre la Casona Universitaria y la Casa Regional de Bolívar.

- El monto para la implementación del enlace de radio frecuencia fue de 2569,74 dólares americanos menor al precio comercial de 4200,00 dólares, por lo que su implementación fue viable por las estudiantes ejecutoras de este trabajo de grado.

- Los datos obtenidos luego de haber realizado el monitoreo están dentro de los parámetros técnicos, normas y estándares establecidas para redes inalámbricas Wi-Fi exigidos para el funcionamiento del enlace (802.11).

- De acuerdo a la evaluación del enlace, la cantidad de Mbps en función del ancho de banda que circulan por el enlace si cumplen con los requerimientos del proyecto, garantizando una transmisión confiable de los datos.

- El radio enlace brinda el servicio de internet a las instancias que laboran en La Casa Regional de Bolívar y ponen a su disposición los nuevos servicios de comunicación para mejorar el desenvolvimiento en las labores cotidianas.

- Tenemos la satisfacción de haber cumplido con nuestro trabajo de grado, el mismo que servirá como un aporte al desarrollo e integración a la red de datos de la Universidad Estatal de Bolívar, al mismo tiempo se brinda el servicio de internet a la comunidad universitaria a través de los Hot-Spot como un valor agregado a nuestro trabajo.

RECOMENDACIONES

- Debido a los cambios brucos de voltaje se recomienda, contar con equipos UPS para asegurar la alimentación eléctrica en los momentos en que está llegue a fallar y prevenir posibles daños en los equipos aprovechando su vida útil.

- Por las condiciones ambientales en las que nos encontramos se recomienda, realizar un mantenimiento periódico de los equipos que se encuentran dentro de las cajas herméticas y las antenas, asegurando de esta manera el correcto funcionamiento del enlace.

- Se recomienda a la universidad a través del Área de Redes y Telecomunicaciones de la Universidad realice un monitoreo constante de los enlaces.

- Para el normal funcionamiento del radio enlace, se recomienda que el manejo de los equipos y software sea realizado por personal capacitado, al no suceder esto se pone en riesgo el funcionamiento del enlace y la vida útil de los equipos.

- Se sugiere acondicionar un lugar adecuado en la Escuela de Sistemas, para el laboratorio de redes con la finalidad de que los estudiantes de la escuela puedan aplicar los conocimientos teóricos en ambientes semejantes a los que en el desarrollo profesional se pudieran encontrar.

- Se debería aumentar el número de horas prácticas para las materias de Arquitectura de Computadores, Redes, Electrónica y Orientación de Tesis

BIBLIOGRAFÍA

1. Leivazea, Francisco. Nociones de Metodología de Investigación Científica. Quito.1996. Págs. 13-14, 17-18.

2. Castro, Miguel, Araceli Lucio, y Rolando Álvarez. Metodología para la elaboración de la tesis de grado. Guayaquil. Primera Edición. 2002. Págs. 73, 76

3. Friendly LLC, Hacker. 2008. Polarización de la antena, Págs. 108-109. Documento en línea disponible en: http://hackerfriendly.com/

4. García Alejandro. 2008. Modelo OSI. Capa de transporte. Págs. 2-3.

5. Comunidad virtual dedica a contenidos de Internet. Cibercursos. 2009. Topologías: Topología en Anillo. Pág. 25. Documento en línea disponible en: http://www.cybercursos.net

6. Otxoa Guilo. 2008. Guía Wireless para todos/as. Pág. 12. Documento en línea disponible en: http://el202.homeip.net/schedule.htm

7. Manual de administración del sistema de Red Hat Enterprise Linux. Capitulo 20. Documento en línea disponible en:

   http://www.gb.nrao.edu/pubcomputing/redhatELWS4/RH-DOCS/rhel-rg-es-4/ch-ftp.html

8. González Jonathan. Diciembre 1998. Teoría de redes informáticas. Capitulo I

9. Ponce Enrique, Enrique Molina, Vicente Mompó. 2009. Redes Inalámbricas IEEE 802.11: Implantación topologías y Configuración. Págs.7- 9.

10. Pelliza Sergio. 2009. Instituto Salesiano de Estudios Superiores: Transmisión de Datos. Pág. 8.

11. Pérez Ignacio. 2007. WIRELESS Redes Inalámbricas WI-FI WLAN: Dispositivos WLAN, Antenas Omnidireccionales. Págs.7-8 y 23.

12. Fonseca Alejandro. Ingeniería en Telemática. Págs. 145-146.

13. Vialfa Carlos. 2008. Seguridades. Filtrado de direcciones Mac. Págs. 47-48.

14. Alfonsin Romina. Rosa Alfonsin, Melisa Castro. 2004. Redes: Introducción. Documento en línea disponible en: http://www.oni.escuelas.edu.ar/2004/SAN_JUAN/730/pag00.HTM

15. Mejía José. 2009. ¿Qué es una red? Documento en línea disponible en: http://ocw.virtualum.edu.co/ocwum/facultad-de-ingenieria-1/redes-i/redes-i/bfque-es-una-red/

16. Gómez Cintia. Silvana Guerra. 2004. ¿Qué es una red? Documento en línea disponible en:http://www.oni.escuelas.edu.ar/2004/SAN_JUAN/730/pag01.HTM

17. Sheldom Tom. 1996. Red LAN. Documento en línea disponible en: http://www.slideshare.net/alexmora/tipos-de-redes-de-telecomunicaciones presentation-764378

18. Universidad de Manizales. Febrero, 2009. Tipos de redes: Red LAN. Documento en línea disponible en: http://ocw.virtualum.edu.co/ocwum/facultad-de-ingenieria-1/redes-i/redes-i/introduccion-a-las-redes/

19. IFLICA. Instalación física y lógica de una red cableada e inalámbrica en un Aula. 2006. Cable de Par Trenzado. Documento en línea disponible en: http://informatica.iescuravalera.es/iflica/gtfinal/libro/index.html

20. Rivera Cristian, Daniel Mora. 2009. Tipo de redes de telecomunicaciones: Red LAN, Red WAN. Documento en línea disponible en: http://www.slideshare.net/alexmora/tipos-de-redes-de-telecomunicaciones-presentation-764378

21. Terra. Juan Villalonga. 2000. Red informática. LAN Inalámbrica. Documento en línea disponible en:http://www.terra.es/personal/lermon/cat/articles/evin0405.htm

22. Kioskea. 2008. Portal informático virtual. Topologías de red. Documento en línea disponible en: http://es.kioskea.net/contents/initiation/topologi.php3

23. Mejía José. 2009. Modelo de referencia OSI. Documento en línea disponible en: http://ocw.virtualum.edu.co/ocwum/facultad-de-ingenieria-1/redes-i/redes i/introduccion-a-las-redes/

24. Taringa. Alberto Nakayama. 2009. Modelo de referencia OSI: Estructura del modelo OSI. Documento en línea disponible en: http://www.taringa.net/posts/apuntes-y-monografias/1301710/Modelo-de-referencia-OSI-,-que-es--como-funka-.html

25. Knabe Virginia. 2008 Modelos de referencia de redes. Documento en línea disponible en: http://www.cs.virginia.edu/~knabe/iic3512/apuntes_3.html

26. Herramientas WEB para la enseñanza de protocolos de comunicación. 2009. Documento en línea disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/modelos/Mtcp.html

27. JuCemax. Subcultura informática virtual. 2009. TCP/IP. Documento en línea disponible en: http://portalhacker.net/index.php/topic,1516.0.html

28. Soto Miguel. 2009. Ingeniería Informática: TCP/IP. Documento en línea disponible en: http://usuarios.lycos.es/janjo/janjo1.html

29. Ivis Suarez, Margelys Hernández, Jesús F. Rumbaut. Axarnet. 2008. Protocolos. Documento en línea disponible en: http://fmc.axarnet.es/redes/tema_06_m.htm

30. Facultad de Informática, Universidad de Murcia. Tutorial y descripción técnica de TCP/IP. Documento en línea disponible en: http://ditec.um.es/laso/docs/tut-tcpip/3376c212.html

31. FACENA. Facultad de Ciencias Exactas y Naturales y Agrimensura. 2009. Protocolos: Implementar IPX. Documento en línea disponible en: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/COMUNW01/Tema_5_Desarrollado.htm

32. Gonzáles Mónica. 2009. Protocolo: NETBIU. Documento en línea disponible en: http://www.investigacion.frc.utn.edu.ar/labsis/Publicaciones/InvesDes/Protocolos-NBI/doc/indice.html

33. Compiladores: Katiuska Reyes, Lusbely Chinchilla, Patricia Blandizzi. Los protocolos de IEEE a nivel físico son: Documento en línea disponible en: http://fmc.axarnet.es/redes/tema_06_m.htm

34. Kioskea. 2009. Portal informático virtual. El protocolo ICMP. Documento en línea disponible en: http://es.kioskea.net/contents/internet/icmp.php3 –

35. Martín.2009. UDP - Protocolos de la familia Internet. Documento en línea disponible en: http://personales.upv.es/rmartin/TcpIp/cap02s11.html

36. Kioskea. 2009. Portal informático virtual. Enrutamiento por Internet. Documento en línea disponible en: http://es.kioskea.net/contents/internet/routage.php3

37. Lycos. Portal Web y buscador. Michael Mauldin.2008. Protocolo FTP y Aplicación. Documento en línea disponible en: http://usuarios.lycos.es/vteforte/ftp.htm

38. Wikibooks. Colección de libros de texto de contenido libre. . 2009. Fundamentos de redes. Componentes de una red. Medios de Transmisión. Documento en línea disponible en: http://es.wikibooks.org/...redes/...red/

39. Lucy Pedro. 2009. Redes Locales UNAD Pasto: Medios de Transmisión guiados. Documento en línea disponible en: http://lucypedrolucia.blog.dada.net/.../MEDIOS+DE+TRANSMISION+GUIADOS

40. Herramienta WEB. Protocolos de comunicación. 2009. Documento en línea disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/fisico/fibra.html

41. Atenea. 2007. Perturbaciones en las transmisiones. Documento en línea disponible en: http://atenea.jpuc.cl/nennio/redes/curso1/noiso.html

42. Escalante Mauro. 2008. Implementación de redes inalámbricas. Estándares de la Industria. Documento en línea disponible en: http://www.readylinkcorp.com

43. García Alejandro. 2007. Estándares de red. Documento en línea disponible en: http://fmc.axarnet.es/redes/tema_05.htm

36. Lozano Alejandro. Redes inalámbricas. Documento en línea disponible en: http://74.125.47.132/search?q=cache:CywFCtfUPPAJ:www.ulavirtual.cl/courses/IINF14/document/Redes_wireless.ppt%3FcidReq%3DIINF14+estandares+de+redes+inalambricas&cd=6&hl=es&ct=clnk&gl=ec

37. Berdinas Celeste, Roberto Testoni. 2009. Antenas: Términos y definiciones. Documento en línea disponible en: http://web.frm.utn.edu.ar/comunicaciones/antenas.html

38. Diccionario Informático. 2009. Hot-Spot. Documento en línea disponible en: http://www.alegsa.com.ar/Dic/hotspot.php

39. Wikipedia. 2009. Enciclopedia libre y políglota. Hot-Spot: Frecuencias y Seguridades. Documento en línea Disponible en: http://es.wikipedia.org/wiki/Hotspot

40. PARAMOWIFIX. Asociación vallisoletana de usuarios de redes inalámbricas 2009. Pigtail. Documento en línea disponible en: http://www.paramowifix.net/antenas/pigtail/index.html

41. Packard Hewlett. 2009. Punto de Acceso: ¿Qué es y para qué sirve un punto de acceso? Documento en línea disponible en: http://www.computadores-y-portatiles.com/punto-de-acceso.html

42. Compostela Wireless. Comunidad virtual para acercar las nuevas tecnologías de comunicación a la comunidad. 2009. Teoría de las Biquad: La Bi-Quad. Documento en línea disponible en: http://www.compostelawireless.net/modules/sections/index.php?op=viewarticle&artid=30

43. D-Link. 2009. ¿Qué es un Punto de Acceso Wireless Wi-Fi 802.11b? Documento en línea disponible en: http://www.34t.com/box-docs.asp?doc=719

44. Barnes Jacobson. 2009. Communication and Cyberspace: Internet. Documento en línea disponible en: www.hipertexto.info/documentos/internet.htm

45. Universidad de Colima. Alejandro Fonseca. 2008. Perturbaciones en la transmisión. Documento en línea disponible en: http://docente.ucol.mx/al058266/PERTURBACIONESENLATRANSMISION.HTML

46. Berkeley. 2009. Internet. Documento en línea disponible en: http://www.sims.berkeley.edu/research/projects/how-much-info2003/internet.htm

47. Black Box Ecuador. 2009. Correo Electrónico. Documento en línea disponible en: http://www.blackbox.ec/index.php?option=com_content&view=article&id=13:funcionamiento-del-correo-electronico&catid=12:soporte&Itemid=28

48. Taringa. Alberto Nakayama. 2009. ¿Qué significa www? Documento en línea disponible en: http://www.taringa.net/posts/.../¿Que-significa-www.html

49. Ciberhabitat. Ciudad de la Informática. 2009. Chat. Documento línea disponible en: http://www.ciberhabitat.gob.mx/cafe/chat/

50. STE DGSCA UNAM. 2009. Subdirección de Tecnología para la Educación. Videoconferencia. Documento en línea disponible en: http://www.coapa.unam.mx/HTML/modDiploDW/pro3gen/martinezv/sitioSTE/conceptovc.htm

51. RIV UAEH. 2009. Sistema de Universidad Virtual. Red institucional de videoconferencia. Documento en línea disponible en: http://virtual.uaeh.edu.mx/riv/videoconferencia.php

52. Tsares. 2009. Technologies Breakingthecircle. VOZ sobre IP. Documento en línea disponible en: http://www.tsares.net/VoIP/FAQ_VoIP.htm

53. OCITEL. Information Technologies. 2008. Concepto de VOZIP. Documento en línea disponible en: http://www.ocitel.net/index.php?option=com_content&view=article&id=52:conceptos-de-voip&catid=39:infotelecom&Itemid=65

54. Álvarez Miguel. 2009. Desarrollo Web: Concepto Telnet. Documento en línea disponible en: http://www.desarrolloweb.com/articulos/telnet-ssh-protocolo-red.html

55. Pillou Jean. 2008. Protocolo Telnet. Documento en línea disponible en: http://es.kioskea.net/contents/internet/telnet.php3

56. Servicios de Internet. 2009. GOPHER Documento en línea disponible en: http://www.usuarios.lycos.es/nhuizar/gopher.htm

57. Barajas Saulo. 2009. Protocolos de seguridad en redes inalámbricas. WPA, WPA2. Documento en línea disponible en: www.saulo.net/pub/inv/SegWiFi-art.htm

58. Tech-FAQ. 2009. Que es la 802.11g.2009. Documento en línea disponible en: http://es.tech-faq.com/802.11g.shtml

59. TECNYO. Revista Online. 2009. Que es un router y para qué sirve. Documento en línea disponible en: http://tecnyo.com/que-es-un-router/

60. Taringa. Alberto Nakayama. 2009. Redes. Concentrador (hub), conmutador (switch) y router. Documento en línea disponible en: http://www.taringa.net/posts/info/1633384/%5BRedes%5D-Concentrador-(hub),-conmutador-(switch)-y-router.html

61. Universidad Técnica Nacional, Facultad Regional Córdova. 2009. Cátedra de Comunicaciones. Introducción a redes, bridge y repetidor. Documento en línea disponible en: http://www.profesores.frc.utn.edu.ar/sistemas/ingcura/Archivos_COM/componentes.asp

62. Kioskea. 2008. Portal informático virtual. Repetidores. Documento en línea disponible en: http://es.kioskea.net/contents/lan/repeteurs.php3

63. MIS RESPUESTAS. 2009. Que es WI-FI. Documento en línea disponible en: http://www.misrespuestas.com/que-es-wifi.html

64. ALMALASI. 2009. WIMAX. Que es y características. Documento en línea disponible en: http://www.configurarquipos.com/doc1087.html

65. PHPBB. 2008. Zona de Fresnel. Documento en línea disponible en: http://gmpg.org/xfn/11

66. WIMAXTECH, Galeon. 2009. Wi-Fi frente a Wimax. Documento en línea disponible en: http://wimaxtech.galeon.com/#%C2%BFQu%C3%A9%20es%20WiMAX

67. Escudero Alberto. 2009. Inicializándose con "radio Mobile" unidad 10.Instalación para exteriores. Documento en línea disponible en: http://www.scribd.com/doc/12786171/Normas-y-Recomendaciones-para-Instalacion-de-Microondas-para-exteriores

68. Lionel Remigio. 2009. Ganancia de una antena. Documento en línea disponible en: http://www.lionelremigio.com/.

69. W3. 2009. Formula de ganancia de una antena: Documento en línea disponible en: http://www.w3.org/TR/xhtml1-transitional.dtd

70. Juan Merlos. 2009. Radiocomunicaciones I. Antenas. Documento en línea disponible en: http://www.merlos.org/radiocomunicaciones/antenas.

GLOSARIO DE TÉRMINOS

AAA.- (Autenticación, Autorización y Administración). Son siglas que se aplican en las herramientas de seguridad.

Ad-hoc.- Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.

ADSL.- Línea de Suscripción Digital Asimétrica. ADSL es un tipo de línea DSL.

ANSI.- Instituto Nacional de Normalización Estadounidense es una organización privada sin fines lucrativos que administra y coordina la normalización voluntaria y las actividades relacionadas a la evaluación de conformidad en los Estados Unidos.

Ancho de banda.- Término que define la capacidad de un canal para acarrear información. En sistemas analógicos, es la diferencia entre la frecuencia más alta que un canal puede acarrear y la menor, medido en hertz.

802.1x.- Estándar de la IEEE que proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves para dispositivos en una red inalámbrica.

ATM.- Modo de Transferencia Asíncrono, proporciona un método de transporte flexible que puede adaptarse a la voz, al vídeo y a los datos.

Banda ancha.- Conexión a Internet de alta velocidad y siempre activa.

Banda de base.-La señal básica directa de salida con base en una frecuencia intermedia obtenida directamente de un dispositivo. Las características de esta señal son la falta de modulación en ésta.

Banda ISM.- Banda de radio utilizada en las transmisiones de redes inalámbricas.

BICSI.- Es una organización con fines no lucrativos y tiene como misión ayudar a los profesionales de las Telecomunicaciones en el desarrollo de sus carreras

proporcionándoles la formación, certificación y publicaciones para el diseño e instalación de tecnologías de voz, datos y video.

Bit (dígito binario).- La unidad más pequeña de información de una máquina.

Bluetooth.- Intenta unir diferentes tecnologías como las de los ordenadores, los teléfonos móviles y el resto de periféricos.

BOOTP: Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

Byte.- Una unidad de datos que suele ser de ocho bits.

CSMA/CA.- (Acceso múltiple de detección de portadora) Un método de transferencia de datos que se utiliza para prevenir una posible colisión de datos.

Cifrado.- Cifrado es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos pueda realizar una interpretación precisa.

Conmutador.- 1. Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.

DDNS.- (Sistema dinámico de nombres de dominio) Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.

Dial up.- Conexión a una línea telefónica a través un módem y una línea telefónica. Es el acceso a internet más económico pero lento.

DHCP.- (Protocolo de configuración dinámica de host) Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

Dispersión de secuencia.- Técnica de frecuencia de radio de banda ancha que se utiliza para la transmisión más fiable y segura de datos.

DNS.- (Servidor de nombres de dominio) La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.

DSL.- (Línea de suscriptor digital) Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.

Dúplex competo.- La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.

Dúplex medio.- Transmisión de datos que puede producirse en dos direcciones a través de una única línea, pero sólo en una dirección cada vez.

EAP.- (Protocolo de autenticación extensible) Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

Enrutador.- Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Enrutamiento estático.- Reenvío de datos de una red a través de una ruta fija.

Ethernet.- Protocolo de red estándar de IEEE que específica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

FCS.- Secuencia de Verificación de Trama, es una trama recibida que tiene una "secuencia" de verificación de trama incorrecta, también conocido como error de CRC difiere de la transmisión original en al menos un bit.

Firewall.- Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

Firmware.- El código de la programación que ejecuta un dispositivo de red. Fragmentación Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.

FTP.- (Protocolo de transferencia de archivos) Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.

Gateways.- Equipos para interconectar redes.

Ghz.- Equivale a 109 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

Gigabyte.- Un GB son 1.024 MB (o MiB), por lo tanto 1.048.576 KB. Cada vez se emplea más el término Gibibyte o GiB.

GSM.- Sistema Global para las Comunicaciones.

Hardware.- El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

HTTP.- (Protocolo de transferencia de hipertexto) Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

Hz (Hercio).- El hertz o hertzio (también se le puede llamar Hercio) es la unidad de frecuencia del Sistema Internacional de Unidades. Existe la división de este término en submúltiplos y múltiplos documentados en un Sistema Internacional de Unidades.

IEEE.- (Instituto de ingenieros eléctricos y electrónicos) Instituto independiente que desarrolla estándares de redes.

IN SITU.- En el lugar, en el sitio.

Infraestructura.- Equipo de red e informático actualmente instalado.

Intervalo de indicador.- El intervalo de frecuencia del indicador, que es una emisión de paquetes de un enrutador para sincronizar una red inalámbrica.

IT.- Tecnologías de la información, es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información.

ITIC.- Carnet Internacional de Profesores, es el documento que cuenta con el respaldo de la UNESCO y de la CAN y que acredita al portador como profesor en todos los países reconocidos por la ISTC.

IP.- (Protocolo Internet) Protocolo utilizado para enviar datos a través de una red.

IPCONFIG.- Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.

ISM.- Industrial, Scientific and Medical, son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia.

ISP.- (Proveedor de servicios de Internet) Compañía que proporciona acceso a Internet.

KB.- (Kilobyte) son 1.024 bytes. (Kilo, proveniente del griego, que significa mil).

Kerberos.- Es un protocolo de seguridad de amplio soporte que utiliza un dispositivo especial conocido como servidor de autenticación. Este revalida contraseñas y esquemas de encriptado. Kerberos es uno de los sistemas de encriptamiento más seguros utilizados en comunicaciones.

LAN.- (Red de área local) Los equipos y productos de red que componen la red doméstica o de oficina.

Login.- El login es el momento de autentificación al ingresar a un servicio o sistema.

LOS.- Línea de Vista Directa, término utilizado en radiofrecuencia para un enlace de radio con visibilidad directa entre antenas.

MAC.- (Dirección de control de acceso al medio) Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

Macintosh.- Es el nombre con el que actualmente nos referimos a cualquier computadora personal diseñada, desarrollada, construida y comercializada por Apple Inc.

Máscara de subred.- Código de dirección que determina el tamaño de la red.

Mbps.- (Megabits por segundo) Un millón de bits por segundo, unidad de medida de transmisión de datos.

Megabyte.- El MB es la unidad de capacidad más utilizada en Informática. Un MB es 1.024 KB, por lo que un MB son 1.048.576 bytes.

Módem.- Es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora.

Modo infraestructura.- Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.

Mhz.- Equivale a 106 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

NAT.- (Traducción de direcciones de red) La tecnología NAT traduce direcciones IP de la red de área local a una dirección IP diferente para Internet.

Navegador.- Programa de aplicación que proporciona una forma de consultar e interactuar con la información de la World Wide Web.

Nodo.- Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.

NLOS.- Sin Línea de Vista Directa, término utilizado en radiofrecuencia para un enlace de radio que no tiene visibilidad directa entre antenas.

Paquete.- Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

PAN.- Las redes inalámbricas de área personal. Las tecnologías PAN más utilizadas son las conexiones por infrarrojos y los módulos de Bluetooth por radio frecuencia, que funcionan en frecuencias de 2,4 GHz sin licencia.

PDA.- (Personal Digital Assistant o Ayudante personal digital) es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red.

PEAP.- (Protocolo de autenticación extensible protegido) Protocolo para la transmisión de de datos de autenticación, incluyendo contraseñas, a través de redes inalámbricas 802.11.

Ping.- (Buscador de paquetes de Internet) Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

PSTN.- Red de telefonía pública conmutada, es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real, garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono.

PoE.- (Alimentación a través de Ethernet) Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente.

POP3.- (Protocolo de oficina de correo 3) Protocolo estándar utilizado para recuperar correo electrónico almacenado en un servidor de correo.

PPTP.- (Protocolo de túnel punto a punto) Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.

Preámbulo.- Parte de la señal inalámbrica que sincroniza el tráfico de red.

Puente.- (Bridge) Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.

Puerta de enlace.- Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.

Puerta de enlace predeterminada.- Dispositivo que redirecciona tráfico de Internet desde su red de área local.

Puerto.- Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

Punto de acceso.- Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

RADIUS.- (Servicio de usuario de marcado con autenticación remota) Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.

RC4 o **ARC4.-** Es el sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas), es muy inseguro por lo que su uso no es recomendable.

Red.- Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

Red Punto a Punto.- Aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos.

Red Punto a Multipunto.- Aquellas en las que cada canal de datos se puede usar para comunicarse con diversos nodos.

Red troncal.- Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos.

Rendimiento.- Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.

Router.- Enrutador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres del nivel de red.

Roaming.- (Vagabundear en español) En comunicaciones inalámbricas, capacidad de un dispositivo de moverse desde una zona de cobertura hacia otra, sin pérdida de la conectividad.

Root.- Raíz. Directorio raíz. En Unix, usuario principal o administrador. Es la cuenta con máximas posibilidades para un usuario en Unix.

Routing.- El proceso de mover un paquete de datos de fuente a destino, normalmente se usa un "Router".

RJ45.- (Registered Jack). El RJ45 es una interfaz física usada para conectar redes de cableado estructurado. Tiene ocho pines, usados generalmente como extremos de cables de par trenzado.

RPC.- Llamada a Procedimiento Remoto es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

Rpm.- Revoluciones por minuto. Unidad de medida para los discos magnéticos.

RTC.- Es un reloj de computadora (generalmente en forma de circuito integrado) que mantiene la hora actual. Los RTCs están presentes en casi todos los dispositivos electrónicos que necesitan del tiempo actual.

RTP.- (Protocolo de tiempo real) Un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.

RTS.- (Solicitud para enviar) Método de red para la coordinación de paquetes grandes a través de la configuración Umbral de solicitud de envío (RTS).

RX.- Abreviatura de Recepción.- Definición de RTP (Real Time Protocol - Protocolo de Tiempo Real). Protocolo empleado para transmitir información en tiempo real como audio y video para una videoconferencia.

SAN.- Red de área de almacenamiento, es una arquitectura para adjuntar dispositivos de almacenamiento de computadoras remotas como un conjunto de discos y conjunto de CDs, como si fuesen dispositivos locales.

Servidor.- Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

SNMP.- (Simple Network Management Protocol - Protocolo simple de administración de red). Protocolo que permite supervisar, analizar y comunicar información de estado entre una gran variedad de hosts, pudiendo detectar problemas y proporcionar mensajes de estados.

Sniffer.- Aplicación de monitorización y de análisis para el tráfico de una red para detectar problemas, lo hace buscando cadenas numéricas o de caracteres en los paquetes.

Software.- Instrucciones para el equipo. Se denomina "programa" al conjunto de instrucciones que realizan una tarea determinada.

SSID.- (Identificador de conjunto de servicio) Nombre de su red inalámbrica.

Telnet.- (Tele Network - Tele Red). Sistema que permite conectarse a un host o servidor en donde el ordenador cliente hace de terminal virtual del ordenador servidor.

TTL.- (Time To Live - Tiempo de Vida). Contador en el interior de los paquetes multicast que determinan su propagación. Es un campo dentro del protocolo IP que especifica cuántos hops (saltos) puede dar un paquete antes de ser descartado o devuelto.

TCP.- (Protocolo de control de transporte) Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TCP/IP.- (Protocolo de control de transporte/Protocolo Internet) Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TFTP.- (Protocolo trivial de transferencia de archivos) Versión del protocolo FTP TCP/IP que utiliza UDP y no dispone de capacidades de directorio ni de contraseña.

TKIP.- (Protocolo de integridad de clave temporal) Protocolo de cifrado inalámbrico que cambia periódicamente la clave de cifrado, haciendo más difícil su decodificación.

TIA/EIA.- Asociación de las industrias de telecomunicaciones. /Asociación de Industrial Electrónicas. Estas dos asociaciones editan normas de forma conjunta, que se conocen como normas TIA/EIA; son las de mayor influencia en el diseño e instalación de redes.

TLS.- (Seguridad de capa de transporte) Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.

Topología.- Distribución física de una red.

TX.- Abreviatura de transmisión.

UDP.- (Protocolo de datagramas de usuario) Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

UMTS.- Servicios Universales de Telecomunicaciones Móviles, busca extender las actuales tecnologías móviles, inalámbricas y satelitales proporcionando mayor capacidad, posibilidades de transmisión de datos y una gama de servicios más extensa.

UNIX.- Sistema operativo multiplataforma, multitarea y multiusuario desarrollado originalmente por empleados de Bell de AT&T, comparten códigos y propiedad intelectual.

URL.- (Localizador uniforme de recursos) Dirección de un archivo situado en Internet.

USB.- Bus Universal en Serie, es un puerto que sirve para conectar periféricos a una computadora.

VPN.- (Red privada virtual) Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.

WAN.- (Red de área extensa) Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.

WEP.- (Protocolo de equivalencia con cable) es un protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que se transmiten de un punto a otro.

WLAN.- (Red de área local inalámbrica) Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.

WPA.- (Acceso protegido Wi-Fi) Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. Asegura la transferencia de datos de forma inalámbrica mediante la utilización de una clave similar a WEP. La robustez añadida de WPA es que la clave cambia de forma dinámica.

WPA2.- (Acceso protegido Wi-Fi 2) es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

ANEXOS

Dr. Rimael Núñez.
DIRECTOR DEL DEPARTAMENTO DE CULTURA DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR.

1. ¿Esté departamento cuenta con el servicio de Internet?

   En la actualidad no contamos con este servicio en este departamento.

2. ¿Han solicitado al Departamento de Internet que les provea de este servicio?

   SI, Hemos conversado con el Dr. Henry Vallejo sobre esta posibilidad y el nos manifestó que este enlace demandaba de una inversión económica fuerte. Por el contrario hemos enviado una solicitud de esté servicio al Vice-Rectorado Administrativo representado por el Ing. Diomedes Núñez, quien nos manifestó de forma verbal que, esta hay la posibilidad de integrar todas las instancias universitarias en un solo enlace el cual estaría inmerso este departamento.

3. ¿Cuál es la forma que emplean para comunicarse con las demás instancias de la Universidad Estatal de Bolívar?

   Por medio del teléfono y personalmente lo hacemos todo.

4. ¿Cuantas líneas telefónicas disponen?

   Disponemos de una sola línea telefónica 2983-120

5. ¿Con cuantas computadoras disponen y cuáles son sus características?
   Contamos con tres computadoras:

   Una Pentium 3, disco duro de 40 GB y 256 de memoria RAM.
   Dos Pentium 4, disco duro de 160 GB y 512 de memoria RAM.

Tecno. Milton Antonio Tapia Nicola.
AYUDANTE DEL MUSEO DE LA ESCUELA DE EDUCACIÓN Y CULTURA ANDINA (EECA).

1. ¿Esté departamento cuenta con el servicio de Internet?

   No contamos con este servicio en esta escuela.

2. ¿Han solicitado al Departamento de Internet que les provea de este servicio?

   Hemos conversado con el Dr. Henry Vallejo sobre esta posibilidad y el nos manifestó que; hubo una intensión de poner un modem para proveernos de este servicio pero no se ha concretado nada.

3. ¿Cuál es la forma que emplean para comunicarse con las demás instancias de la Universidad Estatal de Bolívar?

   Por medio del teléfono, personalmente y contamos con la colaboración del Sr. Eduardo Paredes, quien hace las veces de mensajero y conserje

4. ¿Cuantas líneas telefónicas disponen?

   Disponemos de una sola línea telefónica 2982-013

5. ¿Con cuantas computadoras disponen?

   Contamos con tres computadoras:
   Una Pentium 3 que está en desuso
   Dos Pentium 4 que se encuentran ubicadas en la biblioteca de la Escuela

Dr. Henry Vallejo Ballesteros
DIRECTOR DEL DEPARTAMENTO DE INTERNET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR

1. ¿Qué tipo de conexión a internet tienen en la Casona Universitaria?

   La conexión que tiene la casona universitaria es ADSL

2. ¿Qué tipo de topología de red esta implementada en la casona Universitaria?

   Topología en estrella

3. ¿Cuántas computadoras existen en la Casona Universitaria?

   La casona Universitaria tiene 29 computadoras: 11 computadoras en el laboratorio de computación de Post- Grado; 15 computadoras en las diferentes oficinas, 3 computadoras portátiles para el Programa World Teach.

4. ¿Cuántos equipos activos cuenta la Casona Universitaria?

   Con un router marca TP-LINK

5. ¿Existe alguna infraestructura para redes inalámbrica?

   Si en la parte posterior existe una torre pre-fabricada donde están las antenas de la radio y una antena omnidireccional conectada a un Access Point.

6. ¿Este servicio es libre para la comunidad?

   Es libre para la comunidad universitaria.

7. ¿Qué ancho de banda disponen en la Casona Universitaria?

   512 Mbps

8. ¿Sería factible la implementación de un enlace por radio frecuencia hacia la Casa Regional de Bolívar en el cual se encuentra la Dirección de Cultura de la Universidad, y la Escuela de Educación y Cultura Andina (EECA) de la Facultad de Ciencias de la Educación de la Universidad Estatal de Bolívar?

   Si es factible la implementación del enlace.

Guaranda, 8 de Enero del 2009

Monseñor

ÁNGEL POLIBIO SÁNCHEZ LOAIZA

Obispo de la Diócesis de Guaranda

Ciudad.

De mi consideración:

Me permito en nombre de la Universidad Estatal de Bolívar saludarlo afectuosamente y augurarle éxitos en esté nuevo año; el cual espero sea lleno de dicha y prosperidad.

El motivo de esta carta es el de solicitarle a Usted nos permita colocar una antena para la transmisión de datos e internet en la azotea del edificio de la Curia, la cual nos permitirá integrar inicialmente la Casona Universitaria con el Hospital Antiguo, así como también nos permitirá la navegación inalámbrica en el centro de la ciudad; servicio que se ha dispuesto para toda la comunidad Universitaria (alumnos y docentes). Este trabajo se está efectuando como un proyecto de tesis de ingeniería de sistemas, los equipos instalados son parte de la Universidad

Sabedor de antemano de su alto espíritu de apoyo al desarrollo de las ciencias y de nuestra comunidad, le quedo enormemente agradecido.

Atentamente.

Universidad Estatal de Bolivar
UEB-Net

Dr. Henry Vallejo

Dir. Área Redes y Telecomunicaciones UEB

Recibido.
09-01-2009

DIÓCESIS DE GUARANDA
10 de Agosto 617 y 7 de Mayo Telf. 2981659-
2981639 Fax 2981323 *Guaranda - Ecuador*

Guaranda, 9 de enero de 2009

Doctor
HENRY VALLEJO
Director Área de Redes y Telecomunicaciones de la UEB
Guaranda

De mi consideración:

Reciba un cordial saludo y el deseo de que este nuevo año sea lleno de mucha felicidad y prosperidad, en contestación a su pedido le comunico que estamos dispuestos a colaborar con la instalación de la antena para la transmisión de datos e internet en la azotea de nuestro edificio de la Curia, con los debidos cuidados que este tipo de instalaciones requiere.

Cuando necesite mantenimiento y cuidado de la antena se deberá notificar con anticipación para el permiso necesario.

Atentamente

Mons. Ángel Sánchez Loaiza
OBISPO DE GUARANDA