UNIVERSIDAD AMERICANA DE ACAPULCO

EXCELENCIA PARA EL DESARROLLO

FACULTAD DE INGENIERÍA EN COMPUTACIÓN

INCORPORADA A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CLAVE: 8852-58

~~-~~CONFORMAR E IMPLEMENTAR OPCIONES PARA LA SOLUCIÓN DE REDES INALÁMBRICAS DE BANDA ANCHA EN CAPAMA”

T E S I S

PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

ESCANDÓN VILLAFÁN OMAR.
ROMERO GARCÍA ELENA MONSERRAT.
TUMALÁN MANZANAREZ MARIO.

DIRIGIDA POR:
ING. ÁLVARO LÓPEZ MORALES.

Acapulco Gro. Septiembre del 2010.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ÍNDICE

PÁG.

CAPÍTULO III: TECNOLOGÍA; REDES INALÁMBRICAS (WLAN) CON TECNOLOGÍA CANOPY EN CAPAMA.

CAPÍTULO IV: PROPUESTA DE SOLUCIÓN, DESARROLLO E IMPLEMENTACIÓN EN CAPAMA.

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN.

En la actualidad, los avances tecnológicos han aportado grandes beneficios en nuestra vida diaria, se puede decir que estamos en la era de la información. Los datos, los hechos, las cifras son ya algunos de los bienes más preciados de la humanidad. Pero la información es demasiado abundante; por eso cuanto más rápido y fácil sea el acceso, mejor podremos discriminar cual es importante y cual no.

En una sociedad gobernada por este principio económico y en la que los datos inundan un rincón de nuestras vidas, las redes inalámbricas juegan un papel fundamental y son de hecho las que están haciendo posible que la información en las grandes organizaciones pueda cruzarse, combinarse y contrastarse. En definitiva, permiten agilizar mucho el proceso de toma de decisiones.

Con lo antes mencionado podemos deducir fácilmente que las redes son ya imprescindibles si se quiere tener un acceso rápido y fiable a cualquier tipo de datos, de la misma manera habrá que proteger la información, para el acceso a personas no autorizadas y lo podemos observar a diario, por la explosión de crímenes cibernéticos en todo el mundo. Esta protección no pasará solo por la inclusión de firewalls y otras herramientas para la detección de intrusos en nuestra red, también por la configuración y la administración correcta de nuestros servidores de red. Una definición sencilla de redes inalámbricas es la siguiente; Son aquellas que se comunican por un medio de transmisión no guiado, es decir; sin cables mediante ondas electromagnéticas. La transmisión y la recepción se realizan por medio de antenas. Esto es gracias a los avances tecnológicos de las telecomunicaciones.

El presente documento describe el proceso que se siguió para la solución de redes inalámbricas de banda ancha en CAPAMA (Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco).

En el capítulo I. Presentación del tema: Se plantea el problema, conocer a fondo los obstáculos que hay, para poder resolverlos de una manera eficaz, además de beneficiar y satisfacer las necesidades de CAPAMA, incrementando todos sus movimientos, la seguridad de la información y sobre todo la comodidad de los que diariamente se enfrentan a los problemas del manejo de la información.

En el capítulo II. Marco teórico: Redes y comunicaciones, es una breve reseña acerca de sus antecedentes y algunos conceptos que serán útiles para la realización de este trabajo así como los componentes de una red, sus protocolos, funcionamiento, jerarquías y las distintas topologías.

En el capítulo III. Tecnología: Redes inalámbricas, las tecnologías que ya existen en nuestro campo de trabajo, manejo y la importancia que juegan, el servicio que brinda, sus ventajas y desventajas o distintas opciones que pueden ser implementadas en la misma, así como sugerencias de cómo elaborar una buena red, qué puntos debemos considerar.

En el capítulo IV. Propuesta de solución, desarrollo e implementación en CAPAMA, se presentaran los elementos necesarios para el desarrollo de nuestra solución, su instalación, características de operación, las antenas y todas las herramientas que utilizaremos en los diversos conceptos técnicos para nuestra selección del Hardware necesario, así como el armado y la configuración de la propia red, tratando de beneficiar a los usuarios que utilizan la red y obtener beneficios como grupo de trabajo.

CAPÍTULO I: PRESENTACIÓN DEL TEMA.

1.1 PLANTEAMIENTO DEL PROBLEMA.

En la Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco (CAPAMA), se cuenta con un considerable número de estaciones distribuidas por todo el puerto, en la zona del centro, desde Teniente Azueta sin número, esquina con Quebrada, que se ubica cerca del zócalo de la ciudad, hasta estaciones de cobro y manejo de información en diversas zonas como: Aguas blancas, justo atrás de la central de camiones en avenida ejido, o en capitán Mala Espina atrás del centro comercial Sears de Cuauhtémoc, en la Nao atrás del CICI, también fuera de la ciudad, en la periferia, por ejemplo: En las cruces existe otra estación de cobro, en Walmart y ahora en Diamante y así podríamos continuar mencionando estaciones alrededor de la ciudad de Acapulco.

Estructura de red actual en CAPAMA.

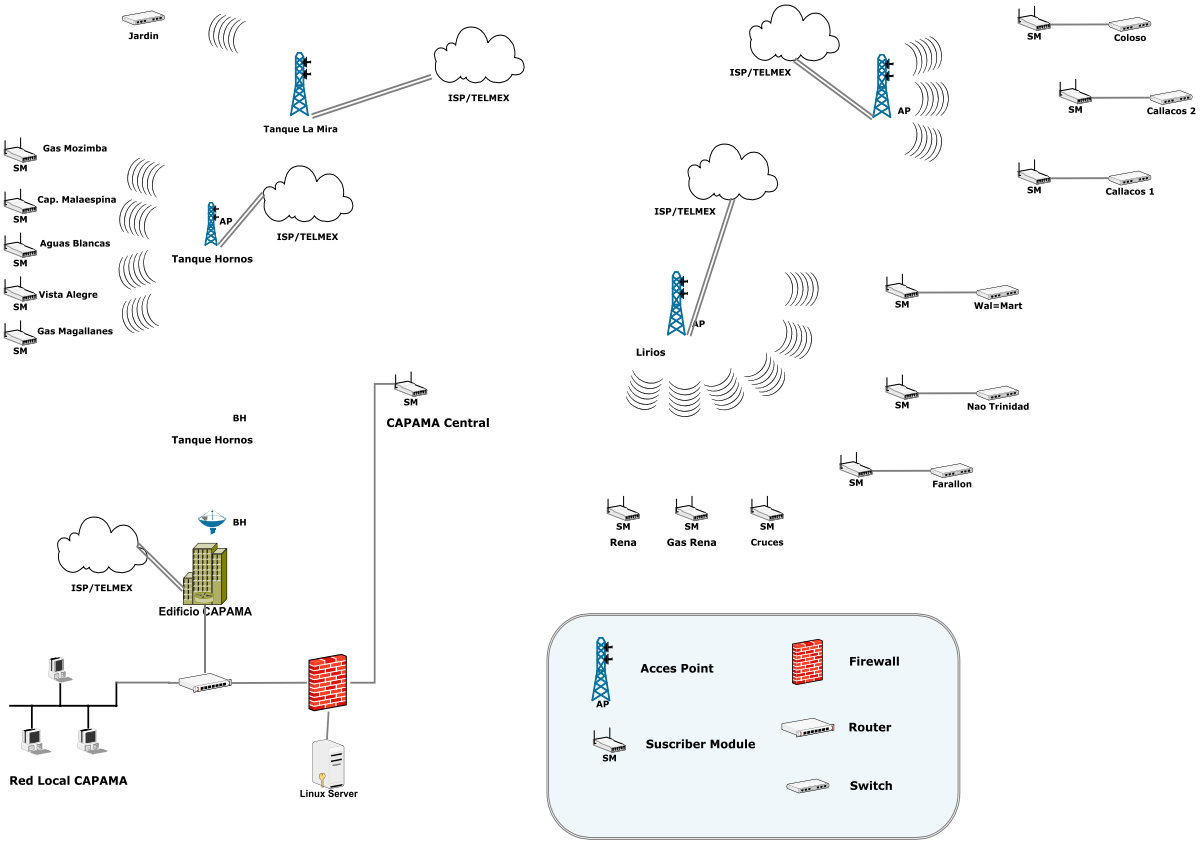

Figura 1- Estructura de red actual en CAPAMA

La imagen anterior (Figura 1) muestra la estructura de red que está funcionando actualmente en CAPAMA y que será reestructurada con una nueva red que satisfaga las peticiones para un óptimo funcionamiento dentro de la institución antes mencionada.

El problema es encontrar la mejor solución posible, para comunicar datos entre las estaciones de CAPAMA, así como los distintos medidores de agua potable, conectados en cerca de 250 puntos situados alrededor de la ciudad, de bajo costo, con un amplio ancho de banda y donde no se pague el uso de espacio radioeléctrico.

Se puede contratar servicio local de internet con Telmex, por ejemplo con Infinitum y utilizar la red de Internet y VPN's para esto, el problema es el costo mensual de éste en cada acceso, es decir; Se tiene que pagar mensualmente la cuota de Internet y datos a Telmex en las distintas estaciones, que según el administrador en informática de CAPAMA son aproximadamente de 56 estaciones distribuidas por el puerto.

Se requiere además la medición de datos en tiempo real con una serie de dispositivos que se están colocando en toda la franja de la costera Miguel Alemán y para los cuales se requeriría otra red adicional, para descargar información al mismo servidor o cablear a una central con todos los riesgos del cableado que esto implica.

Pensar en la solución de Telmex, es impráctico por los costos, además de que se tendría que crear otra red independiente para este tipo de medición en tiempo real, es por ello que en el desarrollo de este trabajo se deberá buscar una solución de redes inalámbricas de bajo costo y un ancho de banda considerable.

1.2 JUSTIFICACIÓN.

Es importante estudiar este problema, al implementar la red inalámbrica de banda ancha con la tecnología CANOPY de Motorola, las estaciones de cobro instaladas en los diferentes puntos del puerto de Acapulco, podrán comunicarse en tiempo real, esto con el fin de no tener perdidas en tiempo para los usuarios en el cobro de los servicios que brinda CAPAMA a la ciudad y brindar mejor servicio a estos al momento de realizar sus pagos, también la ventaja es para agilizar el trabajo en los servicios de acceso a las bases de datos e Internet, entre otras funciones, para los mismos trabajadores de dicha empresa, ya que ahora podemos aprovechar los avances tecnológicos para lograr nuestro objetivo, teniendo una visión a futuro para el crecimiento de CAPAMA, con la novedad de la implementación en la red inalámbrica de banda ancha con tecnología CANOPY.

1.3 OBJETIVOS.

a) Proporcionar Internet a las diferentes estaciones en la Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco (CAPAMA) para la transmisión de datos.

b) Proponer un crecimiento sostenido de la red y poder agregar más nodos y servicios.

c) Definir la infraestructura de la red para beneficio de una mejor comunicación en CAPAMA.

d) Disminuir el costo en la instalación y mantenimiento de la red.

1.4 HIPÓTESIS.

Con la implementación de la red inalámbrica de banda ancha con tecnología CANOPY, mejorará la comunicación entre las estaciones de cobro en tiempo real, el acceso a las bases de datos, entre otros servicios para el beneficio de CAPAMA siendo una de las mejores inversiones de dicha dependencia.

CAPÍTULO II: MARCO TEÓRICO; REDES Y COMUNICACIONES.

2.1 ANTECENDENTES.

En la época de los años setenta y principios de los ochenta, las redes de datos empezaron a obtener importancia, al poder compartir la información en tiempo real, así como diversos recursos. Nadie hubiese imaginado las posibilidades que se abrían hacia un mundo en ese momento inexplorado. Después con los avances de la tecnología, es donde nacen los sistemas de comunicación inalámbrica, primeramente diseñada para comunicación de voz, y después son utilizados para comunicar datos.

Un sistema de comunicación electrónico básico se define como la interconexión entre dos puntos utilizando para ello cualquier medio de transmisión de información. Los sistemas de comunicación electrónica cuentan básicamente con tres etapas principales, el transmisor, que a su vez es también receptor y viceversa, el medio o línea de transmisión.

En los medios de transmisión de datos se ubican varios métodos para enviar información, estos dependen de las señales a transmitir, es decir del tipo de datos a comunicar. Ya que depende también del lugar, puede ser desde cableado estándar, medios fibra óptica o con medios como el aire en donde existen muchas formar de enviar la información, pero en el caso de la comunicación inalámbrica necesitamos algo que se conoce como línea de vista, esto quiere decir que si los puntos a comunicar no se pueden ver entre si, tendremos que colocar puntos intermedios entre ambos para regenerar la señal o buscar algún medio que tenga línea de vista con cualquier punto a comunicar.

2.2 DEFINICIÓN GENERAL DE RED.

Es un sistema de interconexión entre equipos que permite compartir recursos e información. La red se considera como una principal actualización de la tecnología, un ejemplo de una red es el Internet.

Las redes constan de dos o más computadoras conectadas entre si y permiten distribuir recursos e información. La información por compartir suele consistir en archivos y datos, los recursos son los dispositivos o las áreas que se usan como almacenamiento para datos de una computadora, compartida por otra mediante la red. La más simple de las redes es la que conecta dos computadoras, permitiéndoles compartir archivos.

Una red mucho más compleja, conecta todas las computadoras de una empresa o compañía en el mundo, se puede utilizar diversos sistemas de interconexión, por ejemplo, usando como vía los puertos; series y paralelos, estos sistemas baratos no ofrecen velocidad e integridad que necesita un sistema operativo de red seguro y con altas prestaciones que permitan manejar muchos usuarios o recursos.

2.3 COMPONENTES DE UNA RED.

Una red está formada principalmente por computadoras, con sus respectivos periféricos por los elementos de conexión de los mismos y por el Software necesario. Las computadoras pueden desarrollar dos funciones distintas: de servidores o estaciones de trabajo.

Los elementos para la conexión son las tarjetas de red que se encuentran instaladas dentro de una computadora y los cables que las unen. Dentro del Software se puede distinguir sistemas operativos y los protocolos de

comunicación. A continuación se presentan algunos conceptos de los elementos de una red:

SERVIDOR: Este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

ESTACIONES DE TRABAJO: Cuando una computadora se conecta a la red, ésta se convierte en un nodo de la ultima y se trata como una estación de trabajo o cliente. Las estaciones de trabajo pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajo sin discos.

TARJETAS O PLACAS DE INTERFAZ DE RED: Toda computadora que se conecta a una red necesita un dispositivo de estos que soporte un esquema específico, como Ethernet, ArcNet o Token Ring. El cable de red se conectará a la parte trasera de la tarjeta. Los adaptadores o tarjetas actúan como una Interfaz física o conexión entre la computadora y dicho medio de transmisión, estas se colocan en la ranura de expansión en cada computadora. Después de que la tarjeta se ha instalado, se conecta el cable al conector de la misma; para establecer la conexión física entre la computadora y el resto de la red.

Una tarjeta de red realiza las siguientes acciones:

- Prepara los datos de la computadora para su envío a la red, estos se mueven en la computadora, a través del bus, en forma de bits en paralelo y cuando llegan a la tarjeta, los trasmite en serie.

- Envía dichos datos a la red indicando su dirección para distinguirlos de las otras tarjetas de la red.

- Controla el flujo de datos entre la computadora y el sistema de cableado.

- Recibe los datos entrantes en serie del cable y los traduce en bytes en paralelo que el computador pueda comprender.

- Antes de que la tarjeta emisora envié los datos a la red, se establece un dialogo electrónico con la tarjeta receptora: El tamaño máximo de los paquetes de datos que se quieren enviar, el total de estos, el intervalo de tiempo a esperar antes de que sea enviada la confirmación, cuantos datos, la velocidad de transmisión.

SISTEMA DE CABLEADO: El sistema de la red esta constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

RECURSOS Y PERIFERICOS COMPARTIDOS: Entre los recursos compartidos se incluyen dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

2.4 TIPOS DE REDES.

Son varios criterios por los que se pueden clasificar las redes, según su tecnología, su tamaño o topología.

Por su tamaño:

- Se si conectan todas las computadoras dentro de un mismo edificio, se denomina LAN (Local Area Network).

- Si se encuentran en edificios diferentes distribuidos dentro de la misma universidad se llaman CAN (Campus Area Network).

- Si se ubican en edificios diferentes distribuidos en distancias no superiores al ámbito urbano se distinguen como MAN (Metropolitan Area Network).

- Si están instalados en edificios diferentes de la misma o distinta localidad, provincia o país se designan, WAN (Wide Area Network).

Por la forma de conexión:

- Redes sin tarjetas. Utilizan enlaces a través de los puertos serio o paralelo para transferir archivos o compartir periféricos.

- Redes punto a punto. Estos actúan como un conjunto de medios que hace posible la comunicación entre dos computadoras determinadas de forma permanente.

- Redes entre iguales. Todas las computadoras conectadas pueden compartir información con los demás.

- Redes basadas en servidores centrales. Utilizando el modelo básico cliente-servidor.

REDES DE AREA LOCAL (LAN): Es un sistema de comunicaciones con alta velocidad que conecta computadoras y periféricos que se encuentren cerca. Una LAN consta de Hardware y Software de red, sirve para conectar las que están aisladas. Una LAN proporciona la posibilidad de que las maquinas compartan entre sí programas, información y recursos; como unidades de disco, directorios e impresoras de manera que está a disposición a la información de cada puesto y los recursos existentes en otras computadoras. Se puede comparar el Software

que gestiona una red local con el sistema operativo de una computadora, los programas y utilidades que componen el Software de la LAN, actúan como puente de unión entre el usuario y el núcleo central de la computadora. Los programas del Software empleado en una LAN nos permitirán realizar varias actividades, en primer lugar estructurar nuestra computadora, los archivos, las unidades de masa, nombre y código de usuario, etc. Posteriormente entrar dentro del ámbito de la red local, para poder compartir recursos y enviar o recibir mensajes.

Características de las LAN's: El radio que abarca es de pocos kilómetros por ejemplo: Edificios, un campus universitario, un complejo industrial, etc. Utilizan un medio privado de comunicación. La velocidad de transmisión es de varios millones de bps. Pueden atender a cientos de dispositivos muy distintos entre sí (impresoras, computadoras, discos, teléfonos, módems, etc.) ofrecen disponibilidad de comunicación con otras redes a través de pasarelas o Gateways.

RED DE AREA AMPLIA (WAN): Es un sistema de comunicación con alta velocidad que conecta PC's entre sí para intercambiar información, similar a la LAN, sin embargo estos aún no están limitados geográficamente en tamaño. La WAN suele necesitar un Hardware especial, así como líneas telefónicas proporcionadas por una compañía telefónica, también puede utilizar un Hardware y un Software especializado incluir mini y macro- computadoras como elementos de la red. El Hardware para crear una WAN también llega a incluir enlaces de satélites, fibras ópticas, aparatos de rayos infrarrojos y de láser.

2.5 VENTAJAS DE LAS REDES.

- Posibilidad de compartir periféricos costosos como son: impresoras, scanner, fax, etc. Así como también compartir información a través de distintos programas, bases de datos, etc. Con la finalidad que sea más fácil su uso y actualización.

- Reduce e incluso elimina la duplicidad de trabajos.

- Permite utilizar el correo electrónico para enviar ó recibir mensaje de diferentes usuarios de la misma red e incluso de redes diferentes.

- Reemplaza o complementa minicomputadoras de forma eficiente y con un costo bastante reducido.

- Establece enlaces con mainframes. De esta forma, una computadora de gran potencia actúa como servidor haciendo que los recursos disponibles estén accesibles para cada una de las computadoras personales conectadas.

- Permite mejorar la seguridad y control de la información que se utiliza, permitiendo la entrada de determinados usuarios, accediendo únicamente a cierta información o impidiendo la modificación de diversos datos.

- Integración de varios puntos en un mismo enlace.

- Posibilidad de crecimiento hacia otros puntos para integración en la misma red.

- Una LAN posibilita que las PC's compartan entre ellos programas, información, recursos entre otros. La maquina conectada (PC) cambia continuamente, así que permite que sea innovador este proceso y que se incremente sus recursos y capacidades.

2.6 ARQUITECTURA CLIENTE/SERVIDOR.

Al principio de la utilización de las redes, se conectaban las computadoras entre sí para compartir los recursos de todas las que estaban conectadas. Con el

tiempo, los usuarios fueron necesitando acceder a mayor cantidad de información más rápida por lo que fue surgiendo la necesidad de utilizar el servidor.

Un servidor es el que permite compartir sus recursos con las máquinas que están conectadas al servidor. Estos pueden ser de varios tipos y entre ellos se encuentran los siguientes:

- Servidor de archivos. Mantiene los archivos en subdirectorios privados y compartidos para los usuarios de la red.

- Servidor de impresión. Tiene conectadas una o más impresoras que comparte con los demás usuarios.

- Servidor de comunicaciones. Permite enlazar diferentes redes locales o una red local con grandes computadoras o minicomputadoras.

- Servidor de correo electrónico. Proporciona servicios de correo electrónico para la red.

- Servidor Web. Proporciona un lugar para guardar y administrar los documentos HTML que pueden ser accesibles por los usuarios de la red a través de los navegadores.

- Servidor FTP. Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red.

- Servidor Proxy. Se utiliza para monitorizar y controlar el acceso entre las redes. Cambia la dirección IP de los paquetes que manejan cada usuario para ocultar los datos de la red interna a Internet y cuando recibe contestación externa, la devuelve al cliente que la ha solicitado. Su uso

reduce amenazas de piratas que visualicen el tráfico de la red para conseguir la información sobre las computadoras de la red interna.

Según el sistema operativo de red que se utilice y las necesidades que se presenten en una determinada situación, puede ocurrir que los distintos tipos de servidores residan en una misma computadora ó que se encuentren distribuidos entre aquellas que forman parte de la red.

Así mismo, los servidores de archivos pueden establecerse como dedicados o no, según se dediquen solo a la gestión de la red o además se puedan utilizar como estación de trabajo. La convivencia de utilizar uno u otro va estar indicada por la cantidad de estaciones de trabajo que se vayan a disponer, cuanto mayor sea el número de ellas, más conveniente será disponer de un servidor dedicado.

No es recomendable utilizar un servidor no dedicado como estación de trabajo, ya que en caso de que esa máquina tenga algún problema, la totalidad del sistema puede dejar de funcionar por los consiguientes inconvenientes y perdidas irreparables que se pueden producir. El resto de las computadoras de la red se denominan estación de trabajo o clientes y desde ellos se facilita a los usuarios el acceso a los servidores y periféricos de la red.

Cada estación de trabajo es por lo general, una computadora que funciona con su propio sistema operativo. A diferencia de una computadora aislada, la estación de trabajo tiene una tarjeta de red y está físicamente conectada por medio de cables con el servidor.

Distribución de espacio en los discos duros.

En una red el disco o los discos duros pueden ser utilizados de tres maneras distintas: de forma privada, compartida o pública.

Compartición de periféricos.

La principal es compartir la impresora, pretende estar conectada a un servidor para archivos de la red o a un servidor específico denominado servidor de impresión, para esto se dispone un programa que controla los trabajos que se mandan a impresión enviados por los usuarios, este programa crea una zona llamada almacenamiento temporal que guarda datos en el disco y todos los trabajos pendientes por imprimir (cola de impresión), hasta que la impresora quede libre y son dirigidos a ella para ser impresos.

2.7 DOMINIOS Y SERVICIOS DE DIRECTORIO.

Servidor independiente.

En éste, los usuarios tienen excesivas dificultades para localizar sus archivos, impresoras y otros recursos para ser compartidos. Los archivos podrían encontrarse con comandos de MS-DOS, las impresoras se lograrían seleccionar fácilmente de una lista, los usuarios se dan de alta por el administrador de la red y no necesitan tener grandes conocimientos sobre redes.

Los usuarios pueden conectarse e introducir su contraseña para cada servidor y los administradores de redes tienen que estar haciendo llamadas para sincronizar los servidores. También surgirá el problema de que los usuarios recuerden que servidor es el que administra la impresora que van utilizar y en qué lugar se encontraban los archivos que necesita.

Servidor de directorio.

Es una herramienta más en la mejora de la organización de la red. Permiten que un usuario se conecte a la red garantizándose el acceso a los recursos compartidos, sin preocuparse por el servidor donde estén disponibles, en lugar de

tener que conectarse a varios servidores. Los usuarios no necesitan indicar a que servidor se conectan ni en que servidor se encuentra la impresora que quieren utilizar.

Grupos de trabajo.

Son conceptualmente contrarios a los servicios de directorio. Estos grupos son dirigidos por los usuarios cuando reúnen los recursos de sus computadoras. Con una conexión punto a punto, los usuarios comparten los recursos de sus computadoras con otros usuarios. Los usuarios individuales administran los recursos de las computadoras indicando que recursos pueden ser compartidos y cuales tendrán un uso restringido.

Dominios.

Éste fue introducido por Microsoft para Windows NT y toma prestados conceptos de los grupos de trabajo y los servicios de directorio. Los dominios posibilitan dividir redes en redes parciales reducidas, que simplifican el trabajo para la administración. Comprenden un grupo de computadoras, usuarios y recursos que cuentan con una base de datos con seguridad. En la misma manera que los grupos de trabajo, los dominios pueden ser administrados usando una mezcla de controles locales y centrales. Los dominios pueden ser desarrollados fácilmente y con menos planificación que un servicio de directorio.

Los servidores que forman parte de un dominio muestran sus servicios a los usuarios y solo tienen acceso aquellos que poseen permiso. Un servidor puede actuar de tres maneras dentro de un dominio:

- Controlador principal de dominio: Es un servidor en el que almacena la copia muestra de la base de datos para grupos y usuarios del dominio.

- Controlador de reserva de dominio: Es en el que se almacena una copia de seguridad de la base de datos de grupo y usuario del dominio.
- Servidor independiente: Es en el que participan los servidores en un dominio únicamente para compartir sus recursos.

Directorio activo.

Es la implementación de los servicios de directorio para Windows 2000/2003. Su objetivo es ampliar las funciones del sistema de dominios para facilitar la gestión y administración de las redes. Su estructura se basa en los siguientes conceptos:

Dominio: Es la estructura fundamental. Permite agrupar todos los objetos que se administraran de forma estructurada y jerárquica.

Unidad organizativa: Es una unidad jerárquica inferior del dominio que puede estar compuesta por una serie de objetos y por otras unidades organizativas.

Grupos: Son conjuntos de objetos del mismo tipo y se utilizan fundamentalmente para la asignación de derechos para el acceso a los recursos.

Objetos: Es una representación de un recurso de la red (usuarios, computadoras, impresoras, etc.).

2.8 PAQUETES DE DATOS.

La transmisión de datos con una gran extensión en formato de un único bloque no es conveniente y por tanto, los datos a enviar se dividirán en segmentos más pequeños llamados paquetes.

Estos se dividen en cuatro partes:

Cabecera. Esta formada por el identificativo del bloque de comienzo, el identificativo del lugar, destino, origen y la información referente al protocolo que se está utilizando en el paquete.

Información. Contiene el texto o la parte del texto que se trasmite.

Control de errores. Contiene la información necesaria para que el sistema pueda verificar si los datos del paquete se han recibido correctamente.

Bloque final. Contiene la información que indica que el paquete ha finalizado.

Además de estas cuatro partes, también se incluye en cada paquete de datos un número de secuencia, que sirve para que todos los paquetes recompongan el mensaje completo en el orden correcto y permite evitar el envío de paquetes duplicados o la pérdida de alguno.

2.9 CODIFICACIÓN DE DATOS.

En informática, la unidad más pequeña es el bit (dígito binario). La información que contiene son: unos y ceros que se utilizan para indicar si hay presencia o no de carga eléctrica. La unión de ocho bits forma un byte u octeto y es la agrupación básica de información binaria equivalente a un carácter. Para el intercambio de información entre computadoras se han desarrollado distintos sistemas de codificación, como el código ASCII (American Standard Code for Information Interchange), es un código que emplea siete bits más un octavo como control de paridad (bit que se añade en situación 1 ó 0 para que el numero total de bits en situación 1 sea par).

Al principio solo existían 128 códigos (del 0 al 127) que representaban las letras minúsculas y mayúsculas, los números, signos de puntuación y carácteres de control que se usan para instrucciones en impresión. Posteriormente se añadieron los códigos ampliados que contenían carácteres griegos y gráficos, las vocales acentuadas y la Ñ. Actualmente los códigos ASCII son 256 que van desde el 0 al 255.

2.10 NIVELES OSI.

Hablando de protocolos propuestos, destaca el modelo OSI (Open Systems Interconnection), cuya traducción es; Interconexión de Sistemas Abiertos que fue propuesto por la Organización Internacional de Normalización (ISO). Es una organización no gubernamental fundada en 1947, tiene por misión la coordinación del desarrollo y aprobación de estándares a nivel internacional. Su ámbito de trabajo cubre todas las áreas, incluyendo redes locales, a excepción de las áreas electrotécnicas que son coordinadas por IEC (Internacional Electrotechnical Commissión).

El cual propone dividir en niveles las tareas que se llevan a cabo en una comunicación de computadoras. En total se formarían siete niveles como se muestra en la (Figura 2) los primeros cuatro tendrían funciones para comunicación y los tres restantes de proceso, cada uno dispondrán de protocolos específicos para el control de dicho nivel.

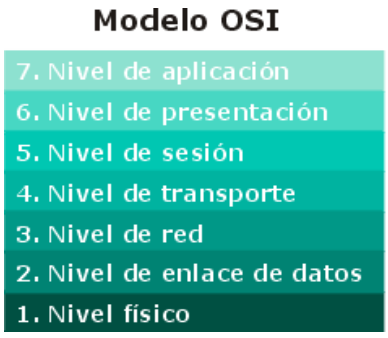

Figura 2 - Modelo OSI

Nivel 1. Físico.

En este nivel se definen las características eléctricas y mecánicas de las redes necesarias para establecer y mantener la conexión física (se incluyen las dimensiones físicas de los conectores, los cables y tipos de señales que van a circular por ellos). Los sistemas de redes locales más habituales definidos en este nivel son: Ethernet, red de anillo con paso de testigo (Token Ring) e Interfaz de datos distribuidos por fibra.

Nivel 2. Enlace de datos.

Se encarga de establecer y mantener el flujo de datos que discurre entre los usuarios. Controla la producción de errores y los corrige (se incluye el formato de los bloques de datos, los códigos de dirección, el orden para los datos transmitidos, la detección y recuperación de errores). Las normas Ethernet y Token Ring también están definidas en este nivel.

Nivel 3. Red.

Decide por donde han de transmitir los datos dentro de la red (se incluye la administración y gestión de los datos, la emisión de mensajes y la regulación del trafico de la red. Entre los protocolos más utilizados definidos en este nivel se encuentran: protocolo Internet (IP Internet protocol) y el intercambio de paquetes entre redes (IPX, Internetwork Packet Exchange) de Novell.

Nivel 4. Transporte.

Asegura la transferencia de la información aún encontrándose fallos que pudieran ocurrir en los niveles anteriores (incluye detección de bloqueos, caídas

del sistema, asegurar la igualdad entre la velocidad de transmisión y recepción, así como también búsqueda de rutas alternativas). Entre los protocolos más utilizados definidos en este nivel se encuentran: El protocolo de control de la trasmisión (TCP transmission control protocol) de Internet, el intercambio secuencial de paquetes (SPX Sequenced Packet Exchange) de Novell y NetBIOS/NetBEUI por Microsoft.

Nivel 5. Sesión.

Organiza las funciones que permiten, que dos usuarios se comuniquen a través de la red (se incluyen las tareas de seguridad, contraseñas de usuarios y la administración del sistema).

Nivel 6. Presentación.

Traduce la información del formato de la maquina por uno comprensible para los usuarios (se incluye el control de las impresoras, emulación de terminal y los sistemas de codificación).

Nivel 7. De aplicación.

Se encarga del intercambio de información entre los usuarios y el sistema operativo (se incluye la transferencia para los archivos y programas de aplicación).

Proceso de la comunicación.

Es el proceso que se produce desde que el usuario envía un mensaje hasta que llega a su destino, consiste en una recorrido a través de todos los niveles (con sus correspondientes protocolos) desde el nivel séptimo, hasta llegar al primero. Ahí se encontrará en el canal de datos y le dirigirá al usuario destino, después volverá a subir por todos los niveles hasta llegar al último de ellos.

2.11 TRANSMISIÓN DE LOS DATOS.

Esto se entiende al proceso de transporte de la información codificada de un punto a otro. En toda transmisión de datos se ha de aceptar la información, convertirla a un formato que se pueda enviar rápidamente y de forma fiable, transmitir datos a un determinado lugar y una vez recibidos de forma correcta, volverlos a convertir al formato que el receptor pueda reconocer y comprender. Todas estas acciones forman el proceso de transmisión, que puede dividir el proceso de transmisión de datos en tres funciones: edición, conversión, control.

- Las funciones de edición dan el formato adecuado a los datos y se encargan de controlar errores.
- Las funciones de conversión se encargan de convertir los datos al formato adecuado.
- Las funciones de control se ocupan del control de la red y del envío y recepción de los mensajes.

Estas funciones se implementan por medio de protocolos.

Medios de transmisión.

Los medios que se utilizan para la transmisión de datos se clasifican en guiados y no guiados. Los medios guiados son aquellos que utilizan un medio sólido (un cable) para la transmisión de datos y los no guiados utilizan el aire para ello: son los medios inalámbricos.

Los cables (medios guiados) transmiten impulsos eléctricos o lumínicos. Los bits se transforman en la tarjeta de red y se convierten en señales eléctricas o lumínicas específicas, que están determinadas por el protocolo que implemente esa red.

La velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los elementos que caracterizan este tipo de medio. La evolución de esta tecnología ha estado orientada por la optimización de estas tres variables.

Existen tres tipos de medios guiados:

1. Par trenzado.
2. Cable coaxial.
3. Fibra óptica.

En la siguiente tabla se muestran las características de los tres tipos de cable (tabla 1).

Tabla 1 - Características de los tipos de cable.

	Par trenzado	Coaxial	Fibra óptica
Ancho de banda	Bajo	Moderado	Muy Alto
Instalación	Sencilla	Fácil	Difícil
Longitud	Baja	Moderada	Muy alta
Costo	Barato	Moderado	Muy caro
Fiabilidad de la transmisión	Baja	Alta	Muy alta
Interferencias	Alta	Moderada	Ninguna
Seguridad	Baja	Baja	Alta
Topología	Bus Estrella Anillo	Bus	Estrella Anillo

Cable de par trenzado.

Este cable consiste en pares de hilos trenzados, recubiertos de una caja aislante externa. Puede ser STP con una impedancia de 120-150 ohmios, o UTP

con una impedancia de 100 ohmios. Los conectores que se utilizan son los denominados RJ45.

En función de sus características se pueden clasificar en cuatro categorías.

Categoría 3. Se utiliza para transmitir datos con una velocidad de transmisión hasta 10 Mbps con longitudes de segmento inferiores a 100 metros y una longitud máxima en la red de 500 metros.

Categoría 4. Se emplea para transmitir datos con una velocidad hasta 16 Mbps.

Categoría 5. Se usa para la transmisión de datos con una velocidad hasta 100 Mbps.

Categoría 6. Se maneja para transmitir datos con una velocidad de hasta 1000 Mbps. Es el más utilizado actualmente.

Cable coaxial.

Es un cable formado por un hilo conductor central rodeado de un material aislante que, a su vez esta rodeado por una malla fina de hilos elaborados por cobre o aluminio a una malla delicada cilíndrica. Todo el cable esta rodeado por un aislamiento que le sirve de protección para reducir las emisiones eléctricas. Se usa normalmente para datos y los sistemas de antenas colectivas para la televisión, transmite una señal con velocidad de transmisión alta. En función de sus características se clasifica en dos categorías:

- Cable coaxial grueso (10BASE5). Tiene un grosor de 0.5 pulgadas, lleva un conector tipo N, alcanza una velocidad de transmisión hasta

10 Mbps y una longitud máxima de 500 metros por el segmento de red. También se designa Tic Ethernet.

- Cable coaxial delgado (10BASE2). Tiene un grosor de 0.25 pulgadas, lleva un conector tipo BNC, alcanza una velocidad de 10 Mbps y una longitud máxima por 200 metros de segmento. También se denomina Thin Ethernet.

Cable de fibra óptica.

Está formado con un cable compuesto por fibra de vidrio (o plástico), cada filamento tiene un núcleo central de fibra de vidrio con un alto índice de refracción que está rodeado por una capa de material similar pero con un índice de refracción menor. De esa manera aísla las fibras y evita que se produzcan interferencias entre filamentos contiguos a la vez que protege al núcleo. Todo el conjunto esta protegido por otras capas aislantes y absorbentes de luz.

Está formado por tres componentes:

- **Transmisor de energía óptica**. Lleva un modulador para transformar la señal electrónica entrante a la frecuencia sometida por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

- **Fibra óptica**. Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

- **Detector de energía óptica**. Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal).

Pueden alcanzar velocidades muy altas a grandes distancias sin necesidad de usar repetidores (el producto de la distancia en kilómetros por la velocidad en Mbps no puede ser superior a 30. Por ejemplo, puede alcanzar una velocidad de 50 Mbps, en una distancia de 600 metros a una velocidad 10 Mbps a 3.000 metros, se ha llegado a conseguir velocidades de 200.000 Mbps.

Medios no guiados.

Se fundamenta en la propagación de ondas electromagnéticas, por el espacio. Una radiación electromagnética tiene una naturaleza dual, como onda y como corpúsculo y su comportamiento dependerá de las características ondulatorias de la radiación, especialmente de la longitud de onda.

Se pueden encontrar los siguientes:

Ondas de radio: Son ondas electromagnéticas cuya longitud de onda es superior a los 30 cm. Son capaces de recorrer grandes distancias y pueden atravesar materiales sólidos, como paredes o edificios. Son ondas multi-direccionales, es decir, se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios. Estas ondas son las que emplean las redes Wi-Fi, Home RF o Bluetooth.

Microondas: Se cimientan en la transmisión de ondas electromagnéticas cuya longitud de onda varía entre 30 centímetros y un milímetro. Estas ondas viajan en línea recta, por lo que el emisor y receptor están alineados cuidadosamente. Tienen dificultades para atravesar edificios debido a la curvatura de la tierra, la distancia entre dos repetidores no debe tener más de unos 80 Km. Es una forma económica para comunicar dos zonas geográficas y mediante un par de torres suficientemente altas para que sus extremos sean visibles.

Infrarrojos: Son ondas electromagnéticas (longitud de onda entre 1 milímetro y 750 nanómetros) direccionales incapaces de traspasar objetos sólidos (paredes). Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología y pueden resultar muy cómodas para máquinas portátiles, sin embargo, no se consiguen altas velocidades de transmisión.

Ondas de luz: Las ondas láser son unidireccionales y se puede utilizar para comunicar dos edificios próximos, instalando en cada uno de ellos un emisor láser y un fotodetector.

2.12 DISPOSITIVOS DE INTERCONEXIÓN.

Entre los equipos que se utilizan para llevar a cabo una transmisión de datos entre distintos equipos para LAN como WAN, se encuentran los siguientes:

Modem: Es un equipo que convierte las señales digitales de una computadora a las analógicas de la línea telefónica (modulación). Las envía a otra computadora y cuando las recibe este, las vuelve a convertir en analógicas a digitales (demodulación).

Modem de cable: Es un dispositivo que permite la provisión de servicios de datos de banda ancha a través de las redes de los operadores de televisión por cable. Los operadores de cable han ofrecido tradicionalmente servicios para la televisión utilizando una infraestructura basada en cable coaxial. Sin embargo, la modernización de estas infraestructuras, ha permitido a dichos operadores proporcionar servicios de datos bidireccionales, especialmente el servicio de conexión a Internet. El inconveniente de este servicio es que el ancho de banda se divide entre el número de usuarios conectados por lo que, a mayor número de usuarios más lenta será la conexión y viceversa.

Modem ADSL: Esta tecnología se utiliza para aprovechar todo el ancho de banda que ofrece el bucle local de abonado y multiplexar las señales de voz y datos. Ofrece lo que se conoce comúnmente como acceso de banda ancha a las redes de datos, especialmente Internet. Su inconveniente es que requiere la adaptación de las infraestructuras de comunicaciones de los operadores, además el uso de éste depende de un factor importante que es la longitud del bucle de abonado, siendo imposible su aplicación para distancias mayores a 5 km.

Repetidor: Es un dispositivo encargado de regenerar la señal en un segmento de una red homogénea ampliando la cobertura. Su forma de actuar es la siguiente: Recoge la señal que circula por la red y la reenvía sin efectuar ningún tipo de interpretación de dicha señal. Son aptos para conectar diferentes medios físicos de transmisión. Sin embargo, no suelen utilizarse para conectar redes de banda base con redes de banda ancha ya que los métodos para la decodificación de la información son muy diferentes.

Concentrador (Hub): Es un equipo que permite compartir el uso de una línea entre varias computadoras. Todas las computadoras conectadas a un concentrador pueden usar la línea pero no de forma simultánea, aún utilizando distintos protocolos y tampoco empleando distintas velocidades de transmisión. El concentrador simplemente regenera y transmite la señal que recibe, pero no es hábil para identificar hacia donde dirige la trama de datos y en función de eso filtrar el tráfico; Tampoco pueden ser empleados para seleccionar la mejor ruta para dirigir las tramas.

Commutador (Switch): Se utiliza igual que un concentrador pero se caracteriza por no enviar los paquetes a todos los puertos, salvo únicamente por el puerto correspondiente al destinatario de los datos. Su función consiste en tomar la dirección MAC destino de una trama de datos (es la dirección que identifica a la tarjeta de red), en función de ella, enviar la información por el puerto correspondiente.

Puente (bridge): Es un sistema formado por Hardware y Software que permite conectar dos redes locales entre si. Se pueden colocar en el servidor de archivos o mejor, en el servidor de comunicaciones. Cuando dos redes locales necesitan comunicarse entre si, necesitan contar con un puente en cada una de ellas para poder conectarse. Ambas redes han de usar el mismo protocolo de comunicaciones.

Encaminador (Router): Éste no solo incorpora la función de filtrado característica de los puentes, sino que además, determina la ruta hacia su destino. Se utiliza tanto en redes de área local como redes de área extensa. Permite la comunicación entre un equipo individual e Internet, entre una red e Internet o entre dos redes, interconecta redes (físicas o lógicas), recibe los paquetes de datos y almacena para distribuirlos progresivamente en función del estado de la red, evita congestión en las redes.

Pasarela (Gateway): Es un sistema formado por Hardware y Software que permite las comunicaciones entre una red local y una computadora de alto rendimiento (mainframe) o un miniordenador (porque utiliza protocolos de nivel transporte, sesión, presentación y aplicación distintos), se suelen colocar en el servidor de comunicaciones.

Cortafuegos (Firewalls): Su función es filtrar los intentos de establecimiento de conexión en tal forma que se pueda detectar e impedir el acceso al sistema para posibles intrusos sin que siquiera se haya llegado a establecer un enlace directo entre ellos. El cortafuego puede ser configurado para permitir que solo determinadas direcciones, origen y destino, puedan acceder a su red.

2.13 INTRODUCCIÓN A LOS PROTOCOLOS.

Un protocolo es una serie de reglas que indican a una terminal como llevar el proceso de comunicación como ya se ha mencionado anteriormente. Por ejemplo: Dos terminales que se comunican pueden tener una arquitectura y sistema operativo diferente que hace imposible la comunicación directa entre ambas. Debido a esto se han desarrollado protocolos que estandarizan la forma en que dos terminales se obligan a establecer comunicación y lo hacen desde cuestiones físicas (por ejemplo: Tipo de cable, niveles de voltaje, frecuencia, etc.) hasta cuestiones de Software (representación de datos, compresión y codificación, entre otras cosas).

Dos elementos que intervienen en el proceso de comunicación lo forman el paquete de información que la terminal transmisora dirige a la terminal receptora, este paquete contiene direcciones, información de usuario e información para corrección de los errores, requeridos para que alcance a la terminal receptora. Además se localiza el protocolo de comunicación.

El protocolo OSI (Open System Interconection) desarrollado por la ISO, el protocolo de la IEEE que de hecho está más orientado al Hardware que al Software y el protocolo TCP/IP originalmente desarrollado por la Secretaria de Defensa de los Estados Unidos de América junto con algunas universidades importantes.

2.13.1 PROTOCOLOS ENCAMINABLES.

Hasta mediados de los ochenta, la mayoría de las redes de área local (LAN) estaban aisladas. Una LAN servía a un departamento o una compañía y rara vez se conectaba con entornos más grandes. Sin embargo, a medida que maduraba la tecnología LAN y la comunicación para los datos necesitaba la expansión de

negocios, las LAN evolucionaron, haciéndose componente de comunicaciones más grandes.

Los datos se envían de una LAN a otra por varios caminos disponibles, es decir, se encaminan a los protocolos que permiten la comunicación LAN a LAN se les conoce como protocolos encaminables. Debido a que los protocolos encaminables se pueden utilizar para unir varias LAN y crear entornos de red para un área extensa, han tomado gran importancia.

2.13.2. JERARQUÍA DE PROTOCOLOS.

La jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía específica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación. Cada nivel tiene su propio conjunto de reglas como se muestra en la (Figura 3.). Los protocolos definen las reglas para cada nivel en el modelo OSI:

Nivel de aplicación	Inicia o acepta una petición.
Nivel de presentación	Añade información de formato, presentación y cifrado al paquete de datos.
Nivel de sesión	Añade información del flujo de tráfico para determinar cuándo se envía el paquete.
Nivel de transporte	Añade información para el control de errores.
Nivel de red	Se añade información de dirección y secuencia al paquete.

Nivel de enlace de datos	Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física.
Nivel físico	El paquete se envía como una secuencia de bits.

Figura 3 - Definiciones de reglas por nivel en el modelo OSI

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los de otros fabricantes, por ejemplo, utilizando NIC (Network Interface card) de varios fabricantes en la misma LAN. Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones. A medida que aumenta el nivel de la jerarquía, también lo hace la sofisticación de las tareas asociadas a los protocolos.

2.13.3 EL PROCESO DE LIGADURA.

El proceso de ligadura (binding process), es con el que se conectan los protocolos entre sí y con la NIC (Tarjeta de Interfaz de Red), permite una gran flexibilidad a la hora de configurar una red. Se pueden mezclar y combinar los protocolos y las NIC según las necesidades. Por ejemplo, se pueden ligar dos jerarquías de protocolos a una NIC, como intercambio de paquetes entre redes e intercambio de paquetes en secuencia (IPX/SPX). Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de ligadura determina la secuencia en la que el sistema operativo ejecuta el protocolo. Cuando se ligan varios protocolos a una NIC, el orden de ligadura es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta. Normalmente, el proceso de ligadura se inicia cuando se instala, se inicia el sistema operativo o el protocolo. Por ejemplo, si el primer

protocolo ligado es TCP/IP, el sistema operativo de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de ligadura.

Las jerarquías de protocolos tienen que estar ligadas o asociadas con los componentes en un orden para que los datos puedan moverse adecuadamente por la jerarquía durante la ejecución. Por ejemplo, se puede ligar TCP/IP a nivel sesión del sistema básico de entrada/salida en red (NetBIOS), así como al controlador de la NIC.

2.13.4 JERARQUÍAS ESTÁNDAR.

La industria informática ha diseñado varios tipos de protocolos como modelos estándar de protocolo. Los fabricantes de Hardware y Software pueden desarrollar sus productos y ajustarse a cada una de las combinaciones de estos protocolos. Los modelos más importantes incluyen:

- La familia de protocolos ISO/OSI.
- La arquitectura de sistemas en red de IBM (SNA).
- Digital DECnet.
- Novell NetWare.
- Apple Talk de Apple.
- El conjunto de protocolos para Internet, TCP/IP.

Los protocolos existen en cada nivel de estas jerarquías, realizando las tareas especificadas por el nivel. Sin embargo, las tareas de comunicación que tienen que realizar las redes se agrupan en un tipo de protocolo entre tres. Cada tipo está compuesto por uno o más niveles del modelo OSI. Antes del modelo de referencia OSI se desarrollaron muchos protocolos. Por tanto, no es extraño

encontrar jerarquías de protocolos que no correspondan directamente con el modelo OSI.

2.13.5 TCP/IP.

El nombre TCP/IP nace por dos protocolos pertenecientes a la familia de protocolos de Internet, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). El TCP/IP esta diseñado para enlazar computadoras de diferentes tipos, incluyendo PCs, minis y mainframes, que ejecuten sistemas operativos distintos, sobre redes de área local y de área extensa; Por tanto, permite la conexión de equipos distantes geográficamente. Otro factor que ha permitido su expansión es la utilización del TCP/IP como estándar de Internet. El mayor problema para TCP/IP estriba en la dificultad de su configuración, por lo que no es recomendable su uso para utilizarlo en una red pequeña.

TCP/IP fué desarrollado en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándose en ARPANET (una red de área extensa del Departamento de Defensa), posteriormente una red dedicada exclusivamente en aspectos militares denominada MILNET después se separó de ARPANET. Fué el germen de lo que después consistiría en Internet.

La arquitectura de TCP/IP transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de los datos. El Internet protocol (IP), un protocolo del nivel de red de OSI, permite a las aplicaciones ejecutarse de forma transparente sobre las redes interconectadas. Las aplicaciones no necesitan conocer que Hardware esta siendo utilizado en la red y por tanto, la misma aplicación puede ejecutarse en cualquier arquitectura de red.

El TCP (Transmission Control Protocol), es un protocolo del nivel de transporte de OSI, asegura que los datos sean entregados, certifica lo enviado con lo recibido y que los paquetes sean reensamblados en el orden en que fueron

mandados. UNIX se empezó a comercializar como el principal sistema operativo que utilizaba TCP/IP y llegaron a ser sinónimos.

2.13.6 PROTOCOLO TCP/IP EN FUNCIONES DE COMUNICACIÓN.

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre computadoras de cualquier tipo ya sea Red o fabricante, respetando los protocolos de cada red individual. Los protocolos TCP/IP se estructuran en cuatro niveles funcionales (Tabla 2):

Tabla 2 - Modelo TCP/IP

APLICACIÓN
TRANSPORTE
RED
FÍSICO

El nivel físico, corresponde al Hardware. Puede ser un cable coaxial, trenzado, fibra óptica o una línea telefónica. TCP/IP no considera oficialmente el nivel físico como componente especifico de su modelo y tiende a agrupar el nivel físico con el de red.

El nivel de red, independientemente del medio físico que se utilice, necesitará una tarjeta de red específica, que a su vez, dependerá del Software llamado controlador de dispositivo proporcionado por el sistema operativo o por el fabricante. Proporciona fiabilidad, en la distribución de datos que pueden adoptar diferentes formatos. El protocolo especifico de este nivel es IP, sin embargo también se encuentran: ICMP, ARP y RARP.

El nivel de transporte, suministra a las aplicaciones con servicios de comunicaciones desde la estación emisora a la receptora. Utiliza dos tipos de

protocolos: TCP que es fiable y orientado a conexión, UDP que no es fiable ni orientado a conexión.

El nivel de aplicación, corresponde a las aplicaciones disponibles para los usuarios como pueden ser: FTP, SN MP, TELNET, etc.

2.13.7 PROTOCOLOS EN NIVEL DE RED.

IP (Internet Protocol) se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por donde se encaminarán los datagramas salientes ofreciendo realizar tareas de fragmentación y reensamblado.

Este protocolo, que no es fiable y también esta orientado a conexión, no garantiza el control de flujo, la recuperación de errores, mucho menos que los datos lleguen a su destino.

IP no se encarga de controlar que sus datagramas que envía a través de la red, puedan perderse, llegar desordenados o duplicados. Para ello tendrán que ser contempladas por protocolos del nivel de transporte. Los datagramas IP contienen una cabecera con información para el nivel IP y datos. Estos datagramas se encapsulan en tramas que dependiendo de la red física utilizada, tiene una longitud determinada. Cuando los datagramas viajan de unos equipos a otros logran atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se utilice para su transmisión. A este tamaño máximo se le denomina MTU (Unidad Máxima de Transmisión) y ninguna red puede transmitir ningún paquete cuya longitud exceda del MTU de dicha red.

Debido a este problema, es necesario reconvertir los datagramas IP en el formato requerido por cada una de las redes que va pasando. Esto es lo que se denomina fragmentación y reensamblado. La fragmentación divide en paquetes

por fragmentos de menor longitud (se realiza en el nivel más inferior posible y de forma transparente al resto de los niveles) y el reensamblado realiza la operación contraria.

ARP (Address Resolution Protocol); Es un protocolo que se utiliza para convertir las direcciones IP en direcciones físicas que puedan ser utilizadas por los manejadores. Para poder realizar esta conversión existe en cada computadora un modulo ARP, que utiliza una tabla de direcciones ARP, en la mayoría de las computadoras aparase como si fuera una memoria intermedia (cache), es decir, la información que lleva mucho tiempo sin utilizarse se borra. Si se encuentra la correspondencia entre la dirección IP y la física se procede a la transmisión.

Si no la encuentra en la tabla, se genera una petición ARP que se difunde por toda la red. Si alguno de las computadoras de la red reconoce su propia dirección IP en la petición ARP, envía un mensaje de respuesta indicando su dirección física y se graba en la tabla de Direcciones ARP.

RARP (Reverse Address Resolution Protocol); Se utiliza cuando, al producirse el arranque inicial, las computadoras no conocen su dirección IP. Requiere que exista en la red, al menos, un servidor RARP. Cuando una computadora desea conocer su dirección IP, envía un paquete que contiene su propia dirección física. El servidor RARP, al recibir el paquete, busca en su tabla RARP, la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete a la computadora origen con esta información. A diferencia del protocolo ARP que se incorpora normalmente en todos los productos TCP/IP, el protocolo RARP solo se incorpora en algunos.

ICMP (Internet Control Message Protocol); Es un protocolo de mantenimiento y gestión que ayuda a supervisar la red. Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino. El objetivo principal de ICMP es proporcionar la información de error o

control entre nodos. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error en este protocolo normalmente los genera y procesa TCP/IP más no el usuario.

Existen cuatro tipos de mensajes ICMP:

- Mensajes de destino no alcanzable.
- Mensajes para el control de congestión.
- Mensajes de redireccionamiento.
- Mensajes de tiempo excedido.

Una de las utilidades de diagnóstico que utiliza este protocolo es la utilidad PING (se utiliza para comprobar si un equipo esta conectado a la red).

2.13.8 PROTOCOLOS EN NIVEL DE TRANSPORTE.

En este nivel se encuentran los protocolos TCP y UDP.

TCP (Transmission Control Protocol); Es un protocolo orientado a conexión que utiliza los servicios del nivel de red. Al igual que cualquier protocolo orientado a conexión, consta de tres fases:

1.- Establecimiento de la conexión. Se inicia con el intercambio de tres mensajes, garantiza que los dos extremos de la transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iniciales de secuencia (cada extremo elige un número de forma aleatoria).

2.- Transferencia de los datos. La unidad de datos que utiliza es el segmento y longitud se mide en octetos. La transmisión es fiable ya que permite la recuperación ante datos perdidos, erróneos o duplicados, así como garantiza la secuencia de entrega, para lo que se añade a la cabecera del segmento de datos

un numero de secuencia y un código de control. La fiabilidad de la recepción se consigue mediante la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.

3.- Liberación de la conexión. Cuando TCP comunica que no tiene más datos que transmitir, éste finaliza la conexión en una dirección. En ese momento TCP, no vuelve a enviar datos en ese sentido, permitiendo que los datos circulen en sentido contrario hasta que el emisor cierra también esa conexión.

TCP permite multiplexación, es decir, una conexión TCP puede ser utilizada simultáneamente por varios usuarios. Como normalmente existe más de un proceso de usuario o aplicación utilizando TCP en forma simultanea, es necesario identificar los datos asociados a cada proceso. Para ello, se utilizan los puertos. Un puerto es una palabra de 16 bits que identifica hacia que aplicación o proceso han de dirigirse los datos.

Hay aplicaciones que tienen asignado el mismo numero de puerto ya que realizan funciones de servidores normalizados que utilizan los servicios TCP/IP. Estos puertos reservados se encuentran en el archivo SERVICES que se encuentra en el directorio ETC y corresponden a números superiores de uno, indicando también si corresponden al protocolo TCP o UDP.

Un socket esta compuesto por un par de números que de forma notable identifican cada aplicación. El socket se compone de dos campos:

1.- La dirección IP de la computadora en el que se esta ejecutando la aplicación.

2.- El puerto a través del cual la aplicación se comunica con TCP/IP.

UDP (User Datagram Protocol); Es un protocolo que se basa en el intercambio de datagramas. Éste concede enviar datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. El inconveniente es que no hay confirmación de recepción, no existe fiabilidad de haber recibido los datagramas en el orden adecuado, debiendo ser la aplicación que se encargue de controlarlo. Al igual que el protocolo TCP, utiliza puertos, sockets y también admite la multiplexación.

2.13.9 PROTOCOLOS A NIVEL DE APLICACIÓN.

Todas las aplicaciones TCP/IP utilizan el modelo cliente/servidor. En este nivel se encuentran un buen número de protocolos los cuales a continuación se describen:

FTP (File Transfer Protocol); Es el más utilizado de todos los protocolos de aplicación. Se utiliza para la transferencia de archivos proporcionando acceso interactivo, también usado para especificaciones de formato y control para la autentificación (es posible conectarse como el usuario anonymous que no necesita contraseña).

HTTP (Hipertexto Transfer Protocol); Es uno de los protocolos más recientes. Se utiliza para manejar la consulta de hipertexto y el acceso a los datos con World Wide Web (WWW). El tráfico generado por este protocolo ha pasado, debido a la influencia de Internet, a ser muy grande.

SMTP (Simple Mail Transfer Protocol); Es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente envía desde una computadora al servidor de otro, pero no específica como se almacena el correo o con que frecuencia se intenta el envío de los mensajes.

SNMP (Simple Network Management Protocol); Sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el trafico de la red desde una o varias estaciones de trabajo llamadas administradores SNMP. Los elementos de la red que puede administrar y monitorizar son dispositivos como computadoras, puertas de enlace (encaminadotes o routers), mainframes, minicomputadoras, conmutador, concentrador, etc.

2.13.10 TELNET.

Permite que un usuario desde una Terminal, acceda a los recursos y aplicaciones de otras computadoras. Una vez que la conexión se encuentra establecida, actúa de intermediario entre ambas computadoras.

Enviando paquetes en la subred local: Una de las responsabilidades de IP es determinar si un paquete puede ser enviado a la subred local o bien debe ser encaminado a otra subred. A continuación se muestran los pasos siguientes:

- IP recibe la trama de TCP que está dirigida a una dirección IP determinada.
- IP compara el identificativo de la subred de la dirección recibida con el identificativo de la subred local. Si ambos coinciden, la trama se envía localmente.
- Antes de proceder al envío local IP debe determinar la dirección de la red física que corresponde a la dirección IP destino. Para ello, utiliza ARP.
- IP añade la siguiente información a la trama.
- La dirección IP origen.
- La dirección física de la red origen.
- La dirección IP destino.
- La dirección física de la red destino.

- IP pasa el paquete con las direcciones añadidas al protocolo de nivel inferior que lo guía a su destino.

2.13.11 PROTOCOLOS NETWARE.

Los cinco protocolos principales utilizados por NetWare son: los protocolos de acceso al medio, definen el direccionamiento que permite diferenciar a los nodos de una red NetWare. El direccionamiento está implementado en el hardware o en la NIC. Las implementaciones más conocidas son:

- 802.5 Token Ring.
- 802.3 Ethernet.
- Ethernet 2.0.

El protocolo es responsable de colocar la cabecera al paquete. Cada cabecera incluye el código del origen y destino. Una vez que se ha transmitido el paquete y está en el medio, cada tarjeta de red comprueba la dirección; si la dirección coincide con la del destino del paquete, o si dicho paquete es un mensaje de difusión, la NIC copia el paquete y lo envía a la jerarquía de protocolos.

- Intercambio de paquetes entre redes/Intercambio de paquetes en secuencia (IPX/SPX, Internetwork Packet Exchange/Sequenced Packet Exchange): define los esquemas de direccionamiento utilizados en una red NetWare, e intercambio de paquetes en secuencia (SPX) proporciona la seguridad y fiabilidad al protocolo IPX. IPX se encuentra a nivel de red basado en datagramas, no orientado a la conexión y tampoco fiable, equivalente a IP, no requiere confirmación por cada paquete enviado. Cualquier control de confirmación o conexión tiene que ser proporcionado por los protocolos superiores a IPX. SPX brinda servicios orientados a la conexión y fiables a nivel de transporte. Novell adoptó el protocolo IPX utilizando el protocolo de

datagramas Internet del Sistema de red de Xerox (XNS). IPX define dos tipos de direccionamiento:

Direccionamiento a nivel red. La dirección de un segmento de la red, identificado por el número de red asignado durante la instalación.

Direccionamiento a nivel de nodo. La dirección de un proceso en algun nodo que está identificado por un número de socket.

Los protocolos IPX sólo se utilizan en redes con servidores NetWare y se suelen instalar con otro conjunto de protocolos como TCP/IP. Incluso NetWare está empezando a utilizar TCP/IP como un estándar.

- Protocolo de información de encaminamiento (RIP). Éste al igual que IPX, facilita el intercambio de información por encaminamiento en una red NetWare y fue desarrollado desde XNS (Xerox Network Service). Sin embargo, en RIP se ha añadido al paquete un campo de datos extra para mejorar el criterio en la decisión para seleccionar la ruta más rápida hasta un destino. El hecho de realizar una difusión de un paquete RIP permite que ocurran ciertas cosas: Las estaciones de trabajo pueden localizar el camino más rápido a un número de red. Los routers pueden solicitar información de encaminamiento a otros routers para actualizar sus propias tablas internas. También consiguen responder a peticiones de encaminamiento en otras estaciones de trabajo o de otros routers y logran asegurarse que si otros routers conocen la configuración de la red y detectar un cambio en la configuración de la red.

- Protocolo de notificación de servicios (SAP, Service Advertising Protocol). Permite a los nodos que proporcionan servicio (incluyen a los servidores como de archivos, impresión, gateway y aplicación), informar de sus servicios y direcciones. Los clientes de la red son hábiles para obtener la

dirección de la red de los servidores a los que pueden acceder. Con SAP, la incorporación y la eliminación de servicios en la red se vuelve dinámica. Por omisión, un servidor SAP informa de su presencia cada 60 segundos.

- Protocolo básico de NetWare (NCP). Define el control de conexión y la codificación de la petición de servicio que hace posible que puedan interactuar los clientes y los servidores. Éste es el protocolo que proporciona los servicios de transporte y sesión. La seguridad de NetWare también está proporcionada dentro de este protocolo.

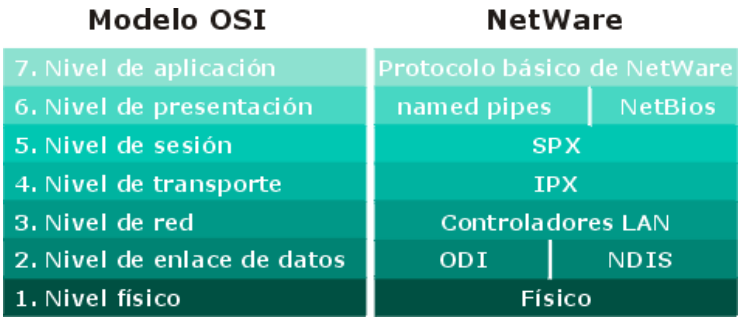

Figura 4 - Comparación del modelo OSI y el modelo NetWare de Novell.

2.13.12 OTROS PROTOCOLOS HABITUALES.

NetBIOS. Resolución de nombres NetBIOS. Cada estación de trabajo en la red tiene uno o más nombres. NetBIOS mantiene una tabla con los nombres y algunos sinónimos. El primer nombre en la tabla es el único de la NIC. Se pueden añadir nombres o usuario opcionales para proporcionar un sistema de identificación expresivo.

Servicio de datagramas NetBIOS. Esta función permite enviar un mensaje a algún nombre, grupo de nombres o a todos los usuarios de la red. Sin embargo, debido a que no utiliza conexiones punto a punto, no se garantiza que el mensaje llegue a su destino.

Servicio de sesión NetBIOS. Este servicio abre una conexión punto a punto entre dos estaciones de trabajo en una red. Una estación inicia una llamada a otra

y abre la conexión. Debido a que ambas estaciones son iguales, pueden enviar o recibir datos concurrentemente.

Estado de la sesión/NIC NetBIOS. Esta función ofrece información sobre la NIC local, otras NIC y las sesiones activas disponibles a cualquier aplicación que utilice NetBIOS. Originalmente, IBM ofrecía NetBIOS como un producto separado, implementado como un programa residente (TSR). Actualmente, este programa TSR es obsoleto; si se encuentra uno de estos sistemas, debería sustituirlo con la Interfaz NetBIOS de Windows.

NetBEUI. Es el acrónimo de Interfaz de usuario ampliada NetBIOS. Originalmente, NetBIOS y NetBEUI estaban unidos y se les consideraba como un protocolo. Sin embargo, varios fabricantes separaron NetBIOS, el protocolo a nivel de sesión, de tal forma que pudiera utilizarse con otros protocolos de transporte encaminables. NetBIOS (Sistema básico de entrada/salida de la red) es una Interfaz para LAN a nivel sesión de IBM que actúa como una Interfaz de aplicación para la red. NetBIOS proporciona a un programa las herramientas para que establezca en la red una sesión con otro programa y debido a que muchos programas de aplicación lo soportan, es muy popular.

Este es un protocolo pequeño, rápido y eficiente a nivel de transporte proporcionado con todos los productos de red por Microsoft. Está disponible desde mediados de los ochenta y se suministró con el primer producto en red de Microsoft: MS-NET. Entre las ventajas de NetBEUI se incluyen su pequeño tamaño (importante para los equipos que ejecuten MS-DOS), su velocidad de transferencia de datos en el medio y su compatibilidad con todas las redes Microsoft.

Sistema red de XEROX (XNS, XEROX NETWORK SYSTEM).

Xerox desarrolló este sistema para sus LAN Ethernet. XNS se utilizaba mucho en los ochenta, pero ha desaparecido lentamente y sustituido por TCP/IP.

Es un protocolo de gran tamaño, lento, ya que genera muchos envíos a todos los dispositivos, aumentando el tráfico de la red.

Comunicación avanzada entre programas (APPC, Advanced Program-to-Program Communication) es un protocolo en nivel transporte de IBM desarrollado como parte de su Arquitectura de Sistemas en Red (SNA). Se diseñó para permitir que los programas de aplicación que se estén ejecutando en distintos equipos lograran la comunicación e intercambio de datos directamente.

Apple Talk.

Es la jerarquía de protocolos en Apple Computer para permitir que los equipos Apple Macintosh compartan archivos e impresoras en un entorno de red. Se introdujo en 1984 como una tecnología LAN autoconfigurable. Apple Talk también está disponible en muchos sistemas UNIX que utilizan paquetes comerciales y con libre distribución. El conjunto de protocolos AppleTalk permite compartir archivos de alto nivel utilizando AppleShare, los servicios y gestores de impresión de LaserWriter, junto con la secuencia de datos en bajo nivel y la entrega de datagramas básicos.

Una colección de protocolos que corresponde con el modelo OSI, soporta:

LocalTalk: Describe el cable par trenzado apantallado utilizado para conectar equipos Macintosh con otros Macintosh o impresoras. Un segmento LocalTalk permite hasta un máximo de 32 dispositivos y opera a una velocidad de 230 Kbps.

Ether Talk: AppleTalk sobre Ethernet. Opera a una velocidad de 10 Mbps. Fast Ethernet opera a una velocidad de 100 Mbps.

Token Talk: AppleTalk sobre Token Ring. Dependiendo de su Hardware, TokenTalk opera a 4 o 16 Mbps.

CAPITULO III: TECNOLOGÍA; REDES INALÁMBRICAS (WLAN) CON TECNOLOGÍA CANOPY EN CAPAMA.

3.1 HISTORIA DE CAPAMA.

En 1946 dentro del periodo presidencial del Lic. Miguel Alemán Valdez se expidió un decreto mediante el cual se creo la primer JUNTA FEDERAL DE MEJORAS MATERIALES (J.F.M.M) en el país con residencia en Acapulco, designando como su presidente al señor Melchor Perusquía, quien con el amplio apoyo económico del gobierno federal interpretó la política oficial desplegando una gran actividad en la construcción de importantes obras materiales entre estas fue resolver el problema del agua, se iniciaron las exploraciones y sondeos en varias zonas de la región, principalmente en el Valle de la Sabana, en donde se encontraron magníficos mantos acuíferos subálveos idóneos para proporcionar agua en cantidades suficientes no solo para satisfacer las necesidades de los habitantes que había entonces, existían volúmenes para incrementos de gastos mayores que pudieran requerirse en el futuro.

Figura 5 - Acapulco en 1950

En 1950 para avanzar rápidamente en los trabajos, la Junta contrato los servicios de gente especializada en hidráulica iniciando en primer término la perforación de 7 Pozos Someros, en la margen derecha del Río de la Sabana imponiendo a la zona el nombre de CAMPO DE POZOS DE AGUA POTABLE (Figura 5). El sistema se mantuvo hasta 1953 año en que la Junta emprendió la perforación de 3 Pozos más, uno de los cuales prestaba servicio exclusivo al poblado de la Sabana; A todo este conjunto de pozos se le llamaba SISTEMA HIDRÁULICO DEL ALTO RIO DE LA SABANA quedando terminado y funcionando normalmente hasta el año de 1960. Desde finales del año 1960 y principios de 1961 en el Valle de la Sabana se tenían en

servicio hasta 16 pozos con una profundidad promedio de 30 metros cada uno, obteniéndose un gasto total de 630 litros por segundo.

Para 1969 la población de Acapulco se multiplico hasta los 174,800 habitantes, solo que las emigraciones fueron precipitadas y sin ningún orden que los asentamientos humanos se ubicaron de forma anárquica principalmente los del área anfiteatro, lo que proporcionó lugar a que se suscitaran problemas de todo tipo, fundamentalmente el relacionado con el del agua potable, drenaje y las aguas pluviales por lo que los tres niveles de gobierno consideraron que era urgente ordenar la reubicación de esos asentamientos humanos. Sorpresivamente las autoridades municipales, con el auxilio de la fuerza pública iniciaron el desalojo del anfiteatro trasladando a los contingentes humanos al Valle de la Sabana para formar la colonia Emiliano Zapata.

Desde ya algún tiempo los técnico en hidráulica y las mismas autoridades habían concluido los estudios realizados, pensando que la única manera de resolver el futuro en Acapulco sería aprovechando las aguas del Río Papagayo, se consolido el interés del Gobierno Federal por un proyecto de esa naturaleza.

Los estudios correspondientes que para tal fin hicieron los técnicos de la Secretaria de Recursos Hidráulicos, contemplaban la posibilidad de un Pozo tipo Ranney con un rendimiento total de 300 litros por segundo y de 12 Pozos Someros; estos 12 pozos aportarían un gasto aproximado de 500 litros por segundo pero con otros 3 pozos más que se construirían después, se llegaría a obtener una producción total de 1,000 litros por segundo. Tal como se proyectaron estas obras así se construyeron denominándosele SISTEMA PAPAGAYO I. Con la construcción de las obras que servirían para mejorar el sistema de agua potable y alcantarillado, Acapulco se transformaría y aceleraría su crecimiento convirtiéndose en el primer puerto turístico de México, con una proyección internacional muy importante.

En el año de 1972 (Figura 6), se desincorporaron los servicios de agua potable y alcantarillado sanitario, creándose una Junta Administradora de Agua Potable y Alcantarillado (J.A.A.P.A.), con el propósito de descentralizar los servicios del Gobierno Federal y lograr una mayor participación ciudadana por parte de los usuarios.

Figura 6 - Acapulco en 1972.

A pesar de que el Gobierno Federal no abandonó su compromiso de dar apoyo para la solución del agua potable al Puerto de Acapulco, durante los años comprendidos entre 1970 y 1974 el organismo administrador del Sistema de Agua Potable y Alcantarillado apenas si podía dar mediano servicio y hacer frente al constante auge de la ciudad.

En 1975 la Secretaria de Recursos Hidráulicos realizó los estudios correspondientes para determinar la factibilidad para construir una nueva captación sobre la margen derecha del Río Papagayo, así como para determinar las obras por realizar y su costo aproximado, tras un análisis de las alternativas obtenidas proponen como solución más adecuada para la captación, la construcción de una obra con toma directa o bocatoma sobre la margen derecha del Río Papagayo a una distancia de un kilómetro aproximadamente aguas abajo del Sistema Papagayo I, denominándose Unidad de Captación PAPAGAYO II.

En el año de 1977, se crea la Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco (CAPAMA) como Entidad Paraestatal de la Administración Publica del Estado.

En 1989, se crea por disposición de la Ley, la Comisión de Agua Potable y Obras Urbanas de Interés Social del Municipio de Acapulco (CAPOUISMA), dicha entidad se convierte en Organismo Público Municipal. El 29 de abril de 1994, por

nuevas reformas a la Ley, retoma la denominación de CAPAMA, con carácter de Organismo Fiscal Autónomo.

En la actualidad CAPAMA es el organismo encargado de surtir agua potable a todo el Municipio de Acapulco, responsabilidad por la cual es muy necesaria una red eficiente de datos y con suficiente ancho de banda para dar servicio a Acapulco.

3.2 LAS REDES INALAMBRICAS WLAN.

Un desarrollo importante en la década pasada es lo relacionado con la tecnología en redes de área local inalámbricas (WLAN Wireless Local Area Network) y aún cuando su propia naturaleza al inicio presentaron problemas diferentes, a través del tiempo han mejorado su operación y rendimiento, a tal grado que los sistemas inalámbricos han tomado gran importancia en las actividades humanas haciéndolas cada vez más comunes.

Al principio las WLAN fueron pensadas para extender o ampliar las redes de área local cableadas en base a equipos portátiles, lo cual permitiría su desarrollo e implementación a mayor velocidad, así como el abatimiento de los costos que implica la modificación de estructuras arquitectónicas.

Las WLAN's son redes que proporcionan conectividad a mayor velocidad en áreas limitadas, tales como edificios u oficinas, además de permitir a los usuarios la libertad para desplazarse dentro del área de cobertura conservando la conexión a la red, es decir, son redes de área local tradicionales a diferencia de que tienen interfaces inalámbricas. Aún con el avance tecnológico, el cual no deja de sorprendernos, esta tecnología tiene ciertas limitantes, por ejemplo, si se utiliza una computadora portátil (laptop) equipada con una tarjeta bajo estándar 802.11 del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), en un radio con mas de 300 metros al aire libre, no es posible establecer conexión, es decir su cobertura

esta limitada. Recordemos que el medio por el cual se comunican los dispositivos inalámbricos es el aire, por lo que al diseñar y planear una red se tiene que considerar los siguientes factores:

1. Ancho de banda /Velocidad de transmisión.
2. Frecuencia de operación.
3. Área de cobertura.
4. Número máximo de usuarios.
5. Aplicaciones que van a utilizarse.
6. Material de construcción de los edificios.
7. Conexión de la WLAN con la red cableada.
8. Disponibilidad de productos en el mercado.
9. Planeación y administración de las direcciones IP.
10. Identificadores de la red (SSID Service Set IDentifier es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red).
11. Seguridad.

Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las WLAN's la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a escenarios públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas con alta densidad de usuarios (hot spots) en las

próximas redes de tercera generación (3G) se observan como las aplicaciones de más interés durante los próximos años.

Muchos de los fabricantes de computadoras y equipos para la comunicación como son los PDA's (Personal Digital Assistants), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLAN's son: Permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

3.3 VENTAJAS DE WLAN SOBRE LAS REDES FIJAS.

Movilidad y libertad de movimientos de los equipos: Las redes inalámbricas proporcionan a los usuarios acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas.

Simplicidad y rapidez en la instalación: La instalación de una WLAN es rápida, fácil y elimina la necesidad de tirar cables a través de paredes y techos.

Flexibilidad en la instalación: La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada, también la misma facilidad con que se instala se desinstala. Esto elimina la necesidad de levantar el cableado existente en el caso de un traslado.

Costo de propiedad reducido: Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en Hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida puede

ser significativamente inferior. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad: Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar, además que resulta cómodo en la incorporación de nuevos usuarios a la red.

Si tenemos los productos adecuados, para crear una red inalámbrica no es nada complicado y si se tiene el soporte correcto aún menos. En una red típica basta con tener las tarjetas inalámbricas para las computadoras, ya sea USB, PCI o PCMCIA; Los puntos de acceso (access points) y verificar que no existan obstáculos muy grandes para logar la transmisión.

Lo más interesante que las WLAN siguen evolucionando y actualmente llegan a velocidades de 108 Mbps, en el estándar 802.11g como en los productos AirPlus XtremeG de DLINK.

3.4 BANDA ANCHA.

En ingeniería de redes se denomina banda ancha a los métodos en donde dos o más señales comparten un medio de transmisión. En telecomunicaciones se le conoce como la transmisión de datos en la cual se envían simultáneamente varios paquetes de información, con el objeto de incrementar la velocidad de transmisión y obtener mejor calidad en servicios en los medios de comunicación audiovisual, VoIP (teléfono por Internet), juegos y servicios interactivos los cuales requieren la transferencia de grandes cantidades de datos.

Existen algunas variantes de los servicios de *línea de abonado digital* DSL (del inglés *Digital Subscriber Line*) como la banda ancha ya que los datos se envía sobre un canal y la voz por otro canal, compartiendo el mismo par de cables.

Los modems analógicos que operan con velocidades mayores a 600 bps también son técnicamente banda ancha, ya que obtienen velocidades de transmisión efectiva mayores usando muchos canales en donde la velocidad para cada canal se limita a 600 baudios. Por ejemplo, un modem de 2400 bps usa cuatro canales de 600 baudios. Este método de transmisión contrasta con la transmisión en banda base, en donde un tipo de señal usa todo el ancho de banda del medio de transmisión, como por ejemplo Ethernet 100BASE-T.

3.5 TÉCNICAS EN REDES INALÁMBRICAS

Actualmente, las técnicas más extendidas para su utilización en redes inalámbricas son: Infrarrojos y Radio.

Infrarrojos: Son ondas electromagnéticas que se propagan en línea recta y que pueden ser interrumpidas por cuerpos opacos. Todas las redes sin hilos por infrarrojos operan usando un rayo de luz infrarroja para transportar los datos entre dispositivos. Estos sistemas necesitan generar señales muy fuertes, debido a que las señales de transmisión dispersas son susceptibles a la luz desde fuentes como ventanas. Puede transmitir señales con alta velocidad en consecuencia al alto ancho de banda de la luz infrarroja (puede emitir a 10 Mbps).

Hay cuatro tipos de infrarrojo:

- Redes en línea de vista (Line-of-sight). Este tipo solo transmite si el transmisor y el receptor se observan limpiamente.
- Redes por dispersión de infrarrojos (Scatter). Este tipo emite transmisiones para que reboten en las paredes, techos y eventualmente contacten con el receptor.
- Redes por reflexión (Reflective). En este tipo, los transceptores ópticos situados cerca de las computadoras transmiten hacia un

punto común que redirige las transmisiones a la computadora apropiada.

- Telepunto óptico de banda ancha. Este tipo proporciona servicios de banda ancha, es capaz de manejar requerimientos de alta calidad multimedia que pueden coincidir con los proporcionados por una red de cable.

No suelen observarse afectados por interferencias externas (con la excepción de la fuerte luz ambiental) y puede alcanzar hasta 200 metros entre el emisor y el receptor. No es necesaria una licencia administrativa para su uso.

Radio. Se pueden distinguir principalmente los siguientes estándares relacionados con las redes inalámbricas.

- IEEE 802.11; Es el estándar para redes WLAN y cubre las funciones del nivel físico. Esta opera en la banda de 2.4GHz, alcanza una velocidad de hasta 54Mbps.
- HiperLAN; El ETSI (European Telecommunications Standars Institute) llevó a cabo durante los años 1991 y 1996 este proyecto con el que pretendía conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11, con una velocidad de transmisión a 23.5 Mbps (54Mbps con HiperLAN/2), muy superior a los 11 Mbps de la actual normativa IEEE 802.11b.
- Bluetooth; Es una tecnología de corto enlace y bajo consumo diseñada para conexión de periféricos a computadora o para dispositivos portátiles. Está optimizada para los transceptores de radio con bajo consumo ideales para los dispositivos personales. Su alcance reducido es bueno para detecciones de proximidad pero como las señales no son suficientemente fuertes para penetrar paredes, suelos o cubrir toda una casa, no es adecuado para redes inalámbricas.

Componentes de las redes inalámbricas:

- Un encaminador para el acceso a Internet.

- Un punto de acceso como mínimo. Es un concentrador inalámbrico, el transmisor/receptor conecta entre si los nodos de la red inalámbrica y normalmente también sirve de puente entre ellos o con la red cableada, un conjunto de puntos de acceso (coordinados) se pueden conectar los unos con otros para crear una red inalámbrica. También proporciona un cable virtual, entre los clientes asociados, este cable inalámbrico conecta tanto a clientes entre si, como a clientes con la red cableada. Este se puede utilizar como repetidor para ampliar la distancia entre los distintos nodos de una red Wi-Fi.

- Clientes inalámbricos. Es cualquier estación que se conecta a una LAN inalámbrica para compartir sus recursos. Una estación se define como cualquier computadora con una tarjeta adaptadora de red instalada que transmite y recibe señales de Radio Frecuencia (RF). Algunos de los clientes inalámbricos más comunes son las computadoras portátiles, PDAs, equipos de vigilancia y teléfonos inalámbricos de voz IP.

3.6 TOPOLOGÍA DE RED.

Se denomina topología a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que las conectan como se muestra en la (Figura 7).

Las estaciones de trabajo en una red se comunican entre sí mediante una conexión física y el objetivo de la topología es buscar la forma más económica y eficaz de conectarlas, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la

red y permitir de forma eficiente el aumento de las estaciones de trabajo. La forma más utilizada actualmente es la configuración en estrella.

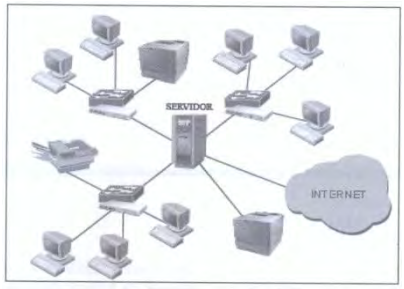

Figura 7 - Topología de red.

Topología en malla:

En esta topología cada dispositivo tiene un enlace dedicado y exclusivo por cada otro dispositivo que forme parte de la red. A pesar de que esta topología es la más eficiente en cuanto a rendimiento es prácticamente inviable en la mayor parte de los casos, ya que es muy cara de implementar y muy compleja de mantener o ampliar.

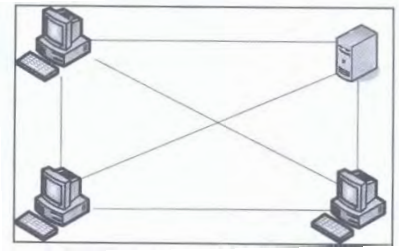

Figura 8 - Topología en malla

Topología en bus:

Es una topología multipunto donde un mismo enlace físico actúa como red troncal que une todos los dispositivos a la red. Esta configuración es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar y disminuir el número de estaciones, el fallo de una estación no repercute en la red, aunque la ruptura de un cable la dejara totalmente inutilizada.

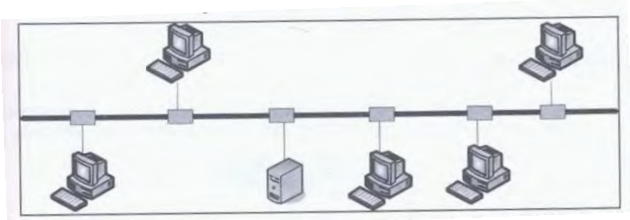

Figura 9 - Topología en bus.

Topología en anillo:

En esta topología cada dispositivo tiene una línea de conexión dedicada y exclusiva solamente con los dos dispositivos más cercanos como se muestra en la (Figura 10). En las primeras redes parecidas a este tipo los datos se movían en una única dirección, de manera que toda la información tenia que pasar por todas las estaciones hasta llegar a la de destino donde se quedaba. Actualmente disponen de dos canales y transmiten en direcciones diferentes por cada uno de ellos.

Este modelo permite aumentar o disminuir el número de estaciones sin dificultad, pero medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.

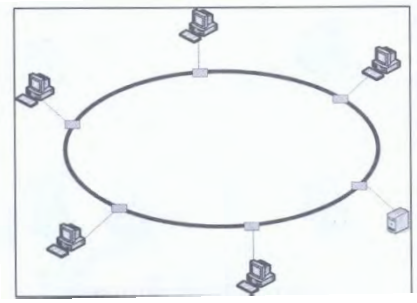

Figura 10 - Topología en anillo.

Topología en estrella:

En esta configuración todos los equipos están conectados directamente al conmutador y las comunicaciones se han de hacer necesariamente a través de el (Figura 11). Permite incrementar y disminuir fácilmente el número de estaciones. Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero si se produce un fallo en el conmutador, la red completa se vendrá abajo.

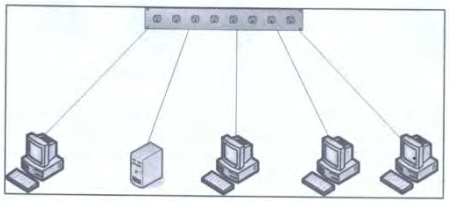

Figura 11 - Topología en estrella.

Topología en árbol:

Esta topología es una variante de la topología en estrella (Figura 12).

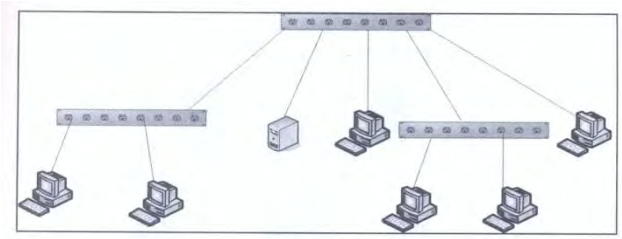

Figura 12 - Topología en árbol.

Topología hibrida:

Se utiliza este término para referirse a la combinación de varias de las topologías anteriores (Figura 13).

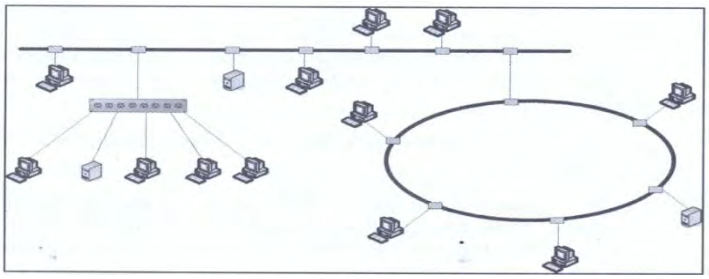

Figura 13 - Topología hibrida.

Topología física y lógica:

Todas las configuraciones que se han estado estudiando hasta ahora son llamadas topologías físicas porque describen como esta extendido el cableado (Figura 14). Además, cada red resigna una topología lógica que describe la red desde la perspectiva de las señales que viajan a través de ella.

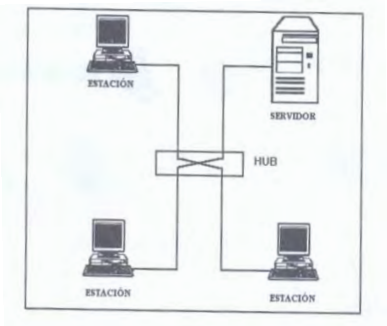

Figura 14 - Topología física y lógica.

Un diseño de red puede tener distinta topología física y lógica (es decir, la forma en que este cableada una red no tiene por que reflejar necesariamente la manera como viajan las señales a través de ella.), a continuación se muestra la siguiente figura.

En ella se muestra una disposición física de configuración en estrella. Cada estación envía y recibe señales por el mismo cable. En el concentrador (**hub**), se mezcla cada señal de las estaciones y son transmitidas a todas ellas (es decir, actúa igual que si estuviera en una configuración en bus). Por tanto, es una topología física de estrella que funciona como una topología lógica tipo bus. Muchas redes nuevas utilizan este modelo ya que es muy fácil de modificar la situación de cada estación (solo hay que desconectar un cable), sin perjuicio para la red entera y además, incrementa las posibilidades en detectar los problemas de red.

3.7 CONFIGURACIÓN DE LA LÍNEA.

Se conoce como configuración de la línea a la forma en la que dos o más dispositivos que comunicados se conectan a un enlace. El enlace es el medio físico por el que se transfieren los datos. En función de esta definición existen dos configuraciones de línea posibles.

- Punto a punto: Cuando exista un enlace dedicado entre dos dispositivos. Toda la capacidad del canal se reserva para la transmisión entre ambos dispositivos (Figura 15).

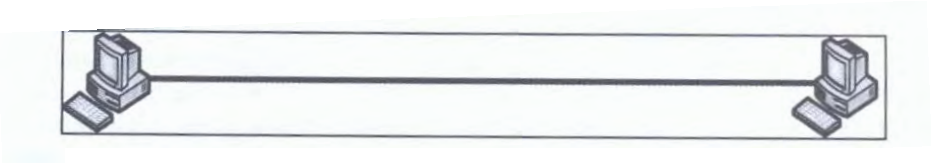

Figura 15 - Configuración de línea (punto a punto).

- Multipunto: Cuando varios dispositivos comparten el mismo enlace, en esta configuración, la capacidad del canal es compartida en el espacio o tiempo (Figura 16).

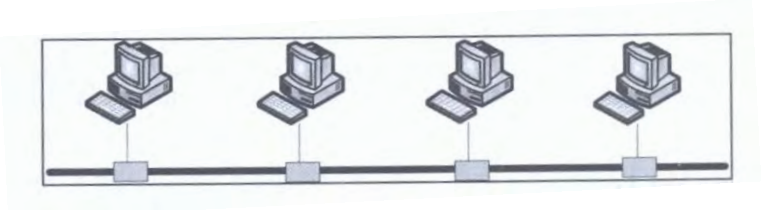

Figura 16 - Configuración de línea (multipunto)

Hay muchos tipos de redes locales, pero las que cuentan con mayor difusión dentro del mundo de las redes: Ethernet, Token Ring.

Ethernet. Esta arquitectura de red fue desarrollada por Xerox Corporation para enlazar un grupo de microcomputadoras, en un principio se creo para ser utilizada con cable coaxial de banda base. Si se utiliza cable coaxial grueso, se obtiene hasta cuatro tramos de cable (unidos con repetidores) y las computadoras se conectan al cable por medio de transceptores. Se logra conectar computadoras en tres tramos únicamente con un máximo de 100 estaciones en cada tramo. Si se utiliza cable coaxial fino, no es necesario utilizar transceptor conectándose el cable a la computadora por medio de una conexión BNC en forma de T. En 1990 el IEEE publico la implementación 10BASE-T (la letra T es de Twisted, trenzado), basada en un elemento central donde se implementa un bus lógico pero utilizando una topología física en estrella. Las uniones entre cada estación y el elemento central se realizan utilizando cable de par.

Fast Ethernet. Esta moderna arquitectura de red esta basada en la tecnología Ethernet, la cual cuenta con las siguientes variaciones que le permiten transmitir a una velocidad de 100 Mbps.

- Esta construida con hubs/Switchs distribuidos que utilizan líneas dedicadas para cada computadora.
- Los cables utilizados son: 100BaseTX, 100 BaseFX y 100BaseT4.
- Se necesitan tarjetas específicas para la velocidad de transmisión a 100 Mbps.

- Utiliza el protocolo de contienda CSMA/CD (Acceso múltiple con detección de portadora y detección a colisiones) y su costo es similar.

Token Ring. Esta arquitectura de red fue creada por IBM en octubre de 1985, sin embargo anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 Kbps y para un máximo de 64 computadoras y una red de banda ancha a 2 Mbps para un máximo de 72 computadoras. Emplea una topología tipo anillo con protocolo de paso a testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica. Los datos se transmiten a una velocidad de 4 Mbps, pudiéndose conectar hasta un máximo de 8 computadoras y a una distancia máxima de 350 metros en cada unidad para acceso multiestación (MAU) si se utiliza con cable coaxial (si se utiliza con fibra óptica puede llegar hasta una velocidad de 16 Mbps).

3.8 SISTEMAS OPERATIVOS DE RED.

Se dividen en dos grupos:

- Sistemas que utilizan el modelo cliente/servidor estos funcionan siendo el esquema de un servidor principal que proporciona soporte a las estaciones de la red. Entre ellos se explicaran: Windows 2000 Server, Windows Server 2003 y Linux.

- Sistemas que utilizan el modelo entre iguales, en ellos no existe un servidor principal, todas las estaciones comparten sus recursos de igual a igual. Entre ellos Windows XP Professional y Windows Vista.

3.9 SISTEMA OPERATIVO LINUX Y SEGURIDAD.

Es un sistema operativo multiusuario con todas las características que necesita tener un sistema operativo moderno esta basado en el sistema operativo Unix, a Linux se le a considerado un clónico de Unix para arquitectura Intel.

Este sistema multiplataforma inicialmente se desarrollo para arquitectura Intel pero con el tiempo se han implementado versiones para otras plataformas. Es un sistema operativo de libre distribución. Esto significa que Linux se distribuye bajo los términos de licencia GPL (General Public License), lo que implica que cualquiera puede libremente copiarlo, cambiarlo y distribuirlo pero sin posibilidad de aplicar restricciones en futuras distribuciones.

Características: Dentro del sistema Linux se maneja con archivos: Desde memoria física del equipo hasta el ratón, pasando por módems, teclado, impresoras o terminales. Esta filosofía de diseño es uno de los factores que más éxito y potencia proporciona a Linux, pero también a uno de los que más peligros entrañan: Un simple error en un permiso puede permitir a un usuario modificar todo un disco duro o leer los datos tecleados desde una terminal. Por esto una correcta utilización de los permisos, atributos y otros controles sobre los archivos es vital para la seguridad de un sistema.

En un sistema Linux típico existen tres tipos básicos de archivos: planos, directorios y archivos especiales o de dispositivos; generalmente, al hablar de archivos se hace referencia a todos ellos, si no se especifica lo contrario. Los archivos planos son secuencias de bytes que no poseen estructura interna ni contenido significante para el sistema: Su significado depende de las aplicaciones que interpretan su contenido. Los directorios son archivos cuyo contenido son otros archivos de cualquier tipo (planos, directorios, o archivos especiales) y los archivos especiales representan dispositivos del sistema; este último tipo se divide en dos grupos; Los dispositivos orientados a carácter y los orientados a bloque. La

principal diferencia entre ambos es la forma al realizar operaciones de entrada/salida, mientras que los dispositivos orientados a carácter las realizan byte a byte (esto es, carácter a carácter), los orientados a bloque realizan en bloques de caracteres.

Cuando un usuario intenta acceder en algún modo a un archivo, el sistema comprueba que terna de permisos es la aplicable y se basa únicamente en ella para conceder o denegar el acceso; Así, un usuario es el propietario del fichero solo se comprueban permisos de la acceso, si no se pasa a la segunda y se aplica en caso de que los grupos coincidan y de no ser así se aplican los permisos de la ultima terna, de esta forma es posible tener situaciones curiosas como la de un usuario que no tenga ningún permiso sobre uno de sus archivos y en cambio que el resto de usuarios del sistema pueda leerlo, ejecutarlo o incluso borrarlo; Obviamente esto no es habitual y de suceder el propietario siempre podrá restaurar los permisos a un valor adecuado.

Seguridad: Podemos entender como seguridad, una característica de cualquier sistema (informático o no) que indica a ese sistema libre de todo peligro, daño o riesgo y que es en cierta manera, infalible.

La confidencialidad dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello y que esos elementos autorizados no convertirán esa información en disponible para otras entidades; La integridad significa que los objetos solo pueden ser modificados por elementos autorizados de una manera controlada y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; Es el contrario de la negación de servicio.

Generalmente tienen que existir tres aspectos descritos para que exista seguridad en un sistema Linux puede conseguir confidencialidad para un

determinado fichero haciendo que ningún usuario (ni siquiera el root) pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Seguridad en las redes inalámbricas: La importancia para implementar la seguridad a una red inalámbrica es por la diferencia de lo que ocurre en las redes cableadas, los datos transferidos a través de redes inalámbricas, utilizan un medio de comunicación que no está restringido, como es el aire. Nuestras datos viajan por un medio de comunicación accesible a cualquier dispositivo externo a la red pero con la capacidad de captación de la señal radioeléctrica, esta característica hace necesario algún método de cifrado de la información que se transmite en una red inalámbrica.

Los mecanismos de prevención más habituales en Linux y en redes son las siguientes:

Mecanismos de autenticación e identificación: Estos mecanismos hacen posible identificar entidades del sistema de una forma única y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quien dice ser). Son los mecanismos más importantes en cualquier sistema ya que forman la base de otros mecanismos que establecen su funcionamiento en la identidad de las entidades que acceden a un objeto.

Mecanismos de control de acceso: Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control al acceso, que controlan todos los accesos sobre el objeto en cualquier entidad del sistema. Dentro de Linux, el control al acceso más habitual es el discrecional (DAC, Discretionary Access Control), implementado por los bits y las listas de control al acceso para cada fichero (objeto) del sistema; Sin embargo, también se permiten especificar controles de acceso obligatorio (MAC).

Mecanismos de separación: Cualquier sistema con diferentes niveles en seguridad deberá implementar mecanismos que permitan separar los objetos en cada nivel, evitando el flujo de información entre objetos y entidades con los diferentes niveles siempre que no exista una autorización expresa del mecanismo de control al acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de cómo separan a los objetos; Separación física, temporal, lógica, criptográfica y fragmentación. Dentro de Linux, el mecanismo de separación más habitual es el de separación lógica o aislamiento, implementado en algunos sistemas mediante una Base Segura de Computo (TCB).

Mecanismo de seguridad en las comunicaciones: Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, se utiliza ciertos mecanismos, la mayoría de los cuales se basan en la criptografía: Cifrado de clave pública, clave privada, firmas digitales, etc. Sin embargo cada vez se utilizan más los protocolos seguros (como SSH o Kerberos), es frecuente encontrar conexiones en texto claro ya no solo entre maquinas de una misma sub red, también en redes diferentes. Una de las mayores amenazas a la integridad de las redes es este trafico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de maquina de la red.

Seguridad en servidores WWW: Hoy en día las conexiones a servidores web son sin duda las más extendidas entre usuarios de Internet, los problemas de seguridad relacionados con el protocolo http se dividen en grupos, los cuales se establecen en función de los datos a los que pueden afectar:

Seguridad en la red: Es necesario garantizar que la información almacenada en la maquina servidora no pueda ser modificada sin autorización,

que permanezca disponible y que solo pueda ser accedida por los usuarios a los que les estén legítimamente permitido.

Seguridad en el cliente: Por ultimo es necesario garantizar al usuario que lo descargado de un servidor no va a perjudicar a la seguridad de su equipo; sin llegar a extremos de applets maliciosos o programas con virus.

Los problemas relacionados con servidores web suelen proceder de errores de programación en los CGI's ubicados en el servidor. Un CGI (Common Gateway Interface) es un código capaz de comunicarse con aplicaciones del servidor, de forma que desde una página se invoque a dichas aplicaciones pasándoles argumentos y el resultado se muestre en el navegador de un cliente; Cuando hacemos un formulario observamos una imagen sensible, o simplemente incrementamos el contador de cierta página, estamos utilizando CGI's. Esta capacidad del CGI para comunicarse con el resto del sistema que alberga las páginas es lo que le otorga su potencia, pero también lo que causa mayores problemas de seguridad.

Los errores más habituales en un CGI provienen de datos recibidos desde el navegador del cliente; Un simple formulario en el que el visitante rellena ciertos campos, puede ser una puerta de acceso a nuestro sistema; Es necesario comprobar validez de todos y cada uno de los datos leídos antes de que sean procesados. Cualquier CGI es susceptible de presentar problemas de seguridad sin importar el lenguaje en que se ha escrito; Por tanto, es revelante preocuparse de mantener actualizado el árbol CGIs (no copiarlo completamente al actualizar la versión de demonio), e incluso revisar los programas en busca de posibles errores.

Otra medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione correctamente, pero nunca como root, recordemos que los CGI's se ejecutan bajo

la identidad del usuario propietario de un demonio, por lo cual si ese propietario es el administrador un potencial atacante podría ejecutar cualquier aplicación como root del sistema.

En ultimo lugar es necesario hablar de la seguridad desde el punto de vista del cliente que visita paginas web; Para el usuario, un servidor es seguro si protege la información que recibe y envía hacia el, manteniendo su privacidad; si no conduce al usuario a descargar programas maliciosos (generalmente virus) en su equipo. También es necesario hablar de los applets hostiles (o simplemente de los mal diseñados) que en muchas ocasiones llegan a detener todas las copias del navegador en memoria; si bien sus implicaciones de seguridad no suelen ser muy graves.

La administración de seguridad en Linux: En Linux los elementos que se encuentran en el sistema de ficheros, es decir, tanto ficheros, como directorios, poseen una serie de características o propiedades que pueden visualizarse con el comando ls-l:

Los campos que aparecen en este listado son los siguientes de la (tabla 3):

Tabla 3 – Características de los ficheros en Linux.

CAMPO	DESCRIPCIÓN
Permisos	Define los permisos sobre el fichero o directorio.
NL	Numero de enlaces del fichero. Si es un directorio, indica el número de subdirecciones.
Prop	Nombre del propietario o dueño del fichero o directorio
Grupo	Nombre del grupo al que pertenece el fichero o directorio
Tam	Tamaño del fichero, en bytes
Fecha y Hora	Indica la fecha y hora de creación o modificación del fichero
Nombre	Nombre del fichero

Permisos	NL	Prop	Grupo	Tam	Fecha	Hora	Nombre
drwxr-xr-x	2	1p	sys	4096	mar 5	02:05	cups
-rw-r—r—	1	root	root	5951	mar 16	01:43	dmesg
drwxr-xr-x	2	root	root	4096	mar 16	01:44	gdm

Como se puede observar en cualquier listado generado por el comando Is, todos los ficheros tienen asociado tanto un nombre de usuario, que es su propietario, como un nombre de grupo. Un grupo es un conjunto de usuarios agrupados para poder establecer permisos de forma conjunta sobre los elementos del sistema de ficheros.

Una de las principales características del sistema de ficheros usado en Linux es que posee un robusto sistema de permisos. Cada fichero del sistema (en directorios) tiene una serie de permisos que definen su accesibilidad a todos los usuarios del sistema. Para ello se utiliza un grupo de 10 carácteres desglosado de la siguiente forma:

-	r w x	r w x	r w x
Tipo	Propietario	Grupo	Otros

El primer carácter indica el tipo de fichero (tabla 4):

Tabla 4 - Tipos de ficheros en Linux.

-	Archivo ordinario
D	Directorio
B	Archivo especial tipo bloque
C	Archivo especial tipo carácter

Los otros nueve carácteres indican, en agrupaciones de tres, los permisos de acceso a ese fichero. La primera agrupación son los permisos al propietario del fichero, la segunda agrupación son los permisos del grupo al que pertenece el

fichero y la ultima agrupación son los permisos del fichero para el resto de usuarios.

Cada agrupación tiene tres carácteres con el siguiente significado:

- Primer carácter: Si aparece una —”rel permiso de lectura sobre el fichero esta activado. Si aparece una ——,significa que no tiene permiso de lectura sobre ese fichero.
- Segundo carácter: Si aparece una —”wel permiso de escritura sobre el fichero esta activado. Si aparece una ——,significa que no tiene permiso de escritura sobre ese fichero.
- Tercer carácter: Si aparece una —”x el permiso de ejecución sobre el fichero esta activado. Si aparece un ——,significa que no tiene permiso de ejecución sobre ese fichero.

3.10 LOCALIZACIÓN Y RESOLUCIÓN DE PROBLEMAS.

Es necesario controlar el rendimiento del sistema revisando ciertos factores como por ejemplo, el tiempo en que tarda el sistema en recuperar programas del disco duro del servidor, en clasificar una base de datos, en ejecutar un programa; guardar un archivo, etc.

Los cambios en el rendimiento ocurren normalmente de forma gradual, no obstante no se notara hasta que sucede algo anormal en la red. Normalmente, debido a la forma de trabajo del sistema operativo de la red, el rendimiento de un disco duro de la red es superior al obtenido con otro tipo de unidades ahora si bien controle de forma periódica el rendimiento del sistema y compare los resultados sucesivos. También será apto de distinguir las variaciones en el rendimiento cuando la red este ocupada al mismo tiempo, los resultados que produzcan podrán ser la primera pista cuando el rendimiento del sistema empiece a

funcionar. Los problemas de funcionamiento de la red que se podrán encontrar pueden depender del Software o del Hardware.

Localización y resolución a problemas de Software. Generalmente los problemas que presenta el Software se originan al no ser instalados de forma adecuada o al utilizar programas monousuario en la red. Normalmente estos problemas afectan solamente algún programa y pueden ocurrirle a uno o a todos los usuarios de dicho programa. Si sospecha que el fallo de funcionamiento es debido a un problema de Software, lo primero que deberá hacer es comprobar los derechos de todos los usuarios que estén teniendo problemas.

Un error común es instalar y probar el software como administrador y como tiene todos los derechos en los directorios puede ocurrir que después se genere algún error al no contar los usuarios con tantos derechos como el. Si los derechos de seguridad no son la causa del problema, entonces se necesita que compruebe la configuración del Software. Muchos de los programas contienen archivos ejecutables y archivos de configuración, así que deben estar localizados en directorios compartidos. Si aun persisten los problemas, necesitamos reinstalar el software en un nuevo subdirectorio y seguir al pie de la letra el manual sin saltar ninguna configuración de la instalación. Si no se soluciona el problema, necesitaremos consultar el distribuidor del programa.

Localización y resolución a problemas de hardware. La localización y reparación de los problemas de Hardware empiezan en la estación de trabajo que produce el error de funcionamiento. Cuando ocurra un problema de Hardware, primero tenemos que inspeccionar la tarjeta adaptadora de la red instalada en la estación de trabajo, así como los cables de la red y las conexiones con la tarjeta.

Comprobación de las tarjetas adaptadoras de red. Si una estación de trabajo falla al colocarse por primera vez en la red, debemos asegurarnos de que la tarjeta esta colocada de forma adecuada en el ordenador. Si la estación sigue

fallando, se deberá comprobar las especificaciones de la tarjeta adaptadora de red o revisar otras tarjetas, como la del ratón, las tarjetas de puerto serie, controladoras, etc. Pueden estar interfiriendo con la tarjeta de red. A veces no podrá conocer las direcciones de las otras tarjetas que existan. En tal caso, la mejor solución es quitar las tarjetas que no sean esenciales. Después tenemos que colocar la tarjeta adaptadora de red en la computadora e intentar conectarse. Si logramos esto, tenemos que empezar a colocar las otras tarjetas, una tras otra e ir probando la conexión cada vez, hasta encontrar la que originó el fallo de la estación de trabajo.

Comprobación de cables. Los primeros problemas de los cables son muy difíciles de diagnosticar. Se sospecha de un problema con un cable, primero comprobaremos que está conectado de forma adecuada con la tarjeta adaptadora de red. Después, revisar si el cable esta partido interrumpirá al acceso de la estación de trabajo a la red. Un cable dañado puede permitir a la estación de trabajo seguir funcionando, pero de forma deficiente. También es posible que fallen las conexiones.

Comprobación del resto de Hardware. El Hardware especifico de la red, las tarjetas y los cables, no son siempre los únicos responsables de los problemas de Hardware. A veces el problema esta en el servidor o en una estación de trabajo. Los tres componentes que tienen más posibilidades de fallo del servidor son la tarjeta controladora del disco, el disco duro y la memoria RAM.

La tarjeta controladora y el disco duro del servidor están constantemente en uso y pueden fallar en cualquier momento. Cuando la tarjeta controladora funciona mal, el servidor puede enviar un mensaje de error si bien a veces no lo hace. Cuando falla el disco duro, siempre aparece un mensaje de error en el momento de arrancar el servidor. Los problemas con la memoria pueden generar algún mensaje. Algunas ocasiones aparecerá un mensaje de error que informa de un

problema en la memoria que produce una paralización del servidor, pero puede que no se repita en un periodo de tiempo.

3.11 TECNOLOGÍA CANOPY.

En el mundo actual las comunicaciones con tecnología de banda ancha, pueden tener buenas demandas los proveedores de servicio no obstante podrían ser abrumadoras. Desde la compra de licencias para instalar y operar redes complicadas que no siempre cumplen las expectativas de los usuarios, hasta tener que competir en un entorno extremadamente difícil y todo esto mientras se esfuerzan por satisfacer las demandas cada vez mayores de los consumidores, esto a consecuencia que muchos pequeños empresarios prefieran dedicarse a otras actividades comerciales. Ahora hablando de tecnologías es aquí cuando mencionamos, el sistema Canopy™, que es la nueva oferta de banda ancha inalámbrica de Motorola, brinda Internet inalámbrico de banda ancha a consumidores y empresas de un modo más rápido, fácil y económico.

Esto es a que la plataforma inalámbrica de Internet con Banda Ancha Canopy de Motorola se despliega fácilmente y es extremadamente económica, por lo que los proveedores de servicio se pueden dedicar por completo a entregar un servicio de alta velocidad y excelente calidad a sus clientes.

Canopy de Motorola no sólo proporciona servicio de banda ancha inalámbrica, sino además minimiza los costos normalmente asociados con las grandes redes de comunicación. Introduce la tecnología de radio al mercado con los proveedores en servicios de Internet. Esta es simplemente la mejor solución para proporcionar a sus clientes Internet de alta velocidad en el tramo final. A continuación se muestra una lista de los modelos de Canopy y sus características:

BackHaul 30.

- Radioenlace digital punto a punto en banda sin licencia (5.4GHz y 5.8 GHz).

- Capacidad Aire de 30 Mbps. Throughput real autoajustable en función de la señal recibida (desde 1.5 Mbps hasta 21 Mbps).
- Distancia de hasta 200 Km LOS y hasta 10 Km NLOS. Interfaz Ethernet.
- Preparados para exteriores con alimentación por POE.
- Suministro con antena integrada o posibilidad de una externa.

BackHaul 60.

- Radioenlace digital punto a punto en banda sin licencia (5.4GHz y 5.8 GHz).
- Capacidad Aire de 60 Mbps. Throughput real autoajustable en función de la señal recibida (desde 3Mbps hasta 43Mbps).
- Distancia de hasta 200 Km LOS y 10 Km NLOS.
- Interfaz Ethernet.
- Preparados para exteriores con alimentación por POE.
- Suministro con antena integrada o posibilidad de una externa.

BackHaul 150.

- Radioenlace digital punto a punto en banda sin licencia (5.4 GHz y 5.8 GHz).
- Capacidad Aire de 150 Mbps. Throughput real autoajustable en función de la señal recibida (desde 4 Mbps hasta 130 Mbps).
- Distancia de hasta 200 Km LOS y 10 Km NLOS.
- Incorpora un canal telefónico E1.
- Interfaz Ethernet.
- Preparados para exteriores con alimentación por POE.
- Suministro con antena integrada o posibilidad de una externa.

BackHaul 300.

- Radioenlace digital punto a punto en banda sin licencia (5.8 GHz).
- Capacidad Aire de 300 Mbps. Throughput real autoajustable en función de la señal recibida (desde 5 Mbps hasta 269 Mbps).

- Distancia de hasta 200 Km LOS y 10 Km NLOS.
- Incorpora 2 canales telefónicos E1.
- Interfaz Ethernet.
- Preparados para exteriores con alimentación por POE.
- Suministro con antena integrada o posibilidad de una externa.

Canopy MP.

- Radioenlace digital punto a multipunto en banda sin licencia (2.4 GHz y 5.4 GHz).
- Configuración Standard o Advantage.
- Capacidad Aire a 10 Mbps. Throughput real de 3-4 Mbps (configuración Standar) y de 14 Mbps (configuración Advantage).
- Interfaz Ethernet.
- Preparados para exteriores con alimentación por POE.
- Suministro con antena integrada. Se estiman distancias máximas de 8 Km para 2.4 GHz y de 3.2 Km en 5.4 GHz.
- Posibilidad de reflector para incrementar distancias. Se estiman distancias máximas de 24 Km para 2.4 GHz y 16 Km para 5.4 GHz.
- Fácil Instalación.

Motorola Mesh. Es una innovadora solución de banda ancha inalámbrica basada en tecnología WiFi, que maximiza el rendimiento, la cobertura y la calidad del servicio con gran aplicabilidad en el mercado y beneficios tanto para el público corporativo como para los usuarios finales. Motorola ya dispone de su innovadora solución para redes Mesh de radios duales, HotZone Dúo (Figura 17). Se trata de una red WiFi Mesh de alto rendimiento, que proporciona acceso de banda ancha inalámbrica escalable y rentable a usuarios residenciales, empresas o municipios, también maximiza el rendimiento, la cobertura esta a la vez, brinda conectividad inalámbrica inigualable,

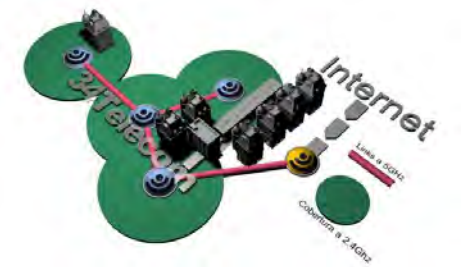

Figura 17 –Solución de tecnología WiFi Motorola Mesh

asegurando un excelente retorno sobre la inversión y satisfaciendo las exigentes realidades económicas del mercado Metro WiFi actual. Con HotZone Dúo se puede proporcionar conectividad a zonas residenciales, a una ciudad completa o a un campus universitario con una red Mesh integrada por varios equipos que conforman una red dinámica auto configurable.

Esto permite a los habitantes de la ciudad tener acceso a muy bajo costo en prácticamente cualquier lugar (casa, oficina, etc.) y también ofrece acceso a banda ancha a los visitantes de la ciudad.

MOTOw¡4, que brinda cobertura IP a prácticamente todos los lugares, incluye soluciones de Banda Ancha Fija, Mesh, Banda Ancha sobre Línea Eléctrica y WiMAX para redes públicas y privadas.

- Red mallada digital en banda sin licencia (2.4 GHz).
- Estructura Multipunto basada en Puntos de Acceso, Repetidores Inalámbricos y Terminales de Abonado que permiten conectividad Mallada (Mesh) entre ellos.
- Capacidad Aire de hasta 6 Mbps.
- Permite roaming y velocidades superiores a 200 KM/h.
- Interfaz Ethernet.
- Disponibilidad de tarjetas tipo PCMCIA para terminales abonados de última milla.

Motorola Moscad y Moscad_ L.

- Unidad Remota de Telecontrol, sistema de entradas salidas modular y sistema de comunicaciones totalmente integrado.
- Producto: MOSCAD_M: Unidad Remota de Telecontrol, sistema compacto y de bajo consumo.

Los productos de red inalámbrica de Motorola son líderes mundiales en este segmento y disponen de una excelente reputación entre los profesionales, la gama se divide en dos líneas básicas:

- **Wireless Mesh Networks.**
  Productos para redes inalámbricas malladas (mesh) donde los dispositivos son interdependientes.
- **Canopy Solutions.**
  Productos para redes inalámbricas tradicionales y para conexiones punto a punto de altas prestaciones.

3.12 ANTENAS PARA REDES INALÁMBRICAS.

Las antenas de redes inalámbricas se pueden dividir en tres tipos:

- **Antenas direccionales (directivas).**

  Orientan la señal en una dirección muy determinada con un haz de luz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite una luz concreta y estrecha pero de forma intensa (más alcance).

  Las antenas direccionales envían la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se escucharía nada, es decir no se puede establecer comunicación entre los interlocutores.

  El alcance de una antena direccional es determinado por una combinación de los dBi de ganancia de la antena, la potencia en emisión del punto y acceso al emisor y la sensibilidad a la recepción del punto de acceso receptor.

- **Antenas omnidireccionales.**

  Orientan la señal en todas direcciones con un rayo amplio pero de corto alcance. 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.

  Las antenas omnidireccionales envían la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. 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 con los dBi en ganancia de la antena, la potencia al emitir del punto de acceso emisor y la sensibilidad en recepción al punto de acceso receptor. A mismos dBi, una antena sectorial o direccional proporcionará mejor cobertura que una omnidireccional.

- **Antenas sectoriales.**

  Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un rayo más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal.

  Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) se deberán instalar tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

- **Apertura vertical y apertura horizontal.**

La apertura es cuanto se abre el haz de luz de la antena. El rayo emitido o recibido por antena tiene una abertura determinada verticalmente y otra apertura determinada horizontalmente.

En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y 40º, la antena sectorial oscilará entre los 90º y los 180º.

En la apertura se deberá tener en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia (potencia por decirlo de algún modo) menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales.

CAPÍTULO IV: PROPUESTA DE SOLUCIÓN, DESARROLLO E IMPLEMENTACIÓN EN CAPAMA.

4.1 PROPUESTA DE SOLUCIÓN.

Nuestra propuesta es encontrar una tecnología de bajo costo, para la implementación de la red inalámbrica en la dependencia, el sistema de red debe ser confiable, también tendremos que pensar en un proveedor de suficiente prestigio en el mercado de las telecomunicaciones, que posea redes inalámbricas de banda ancha, económicas y que no se deba pagar el uso de frecuencias, buscando eficiencia y economía.

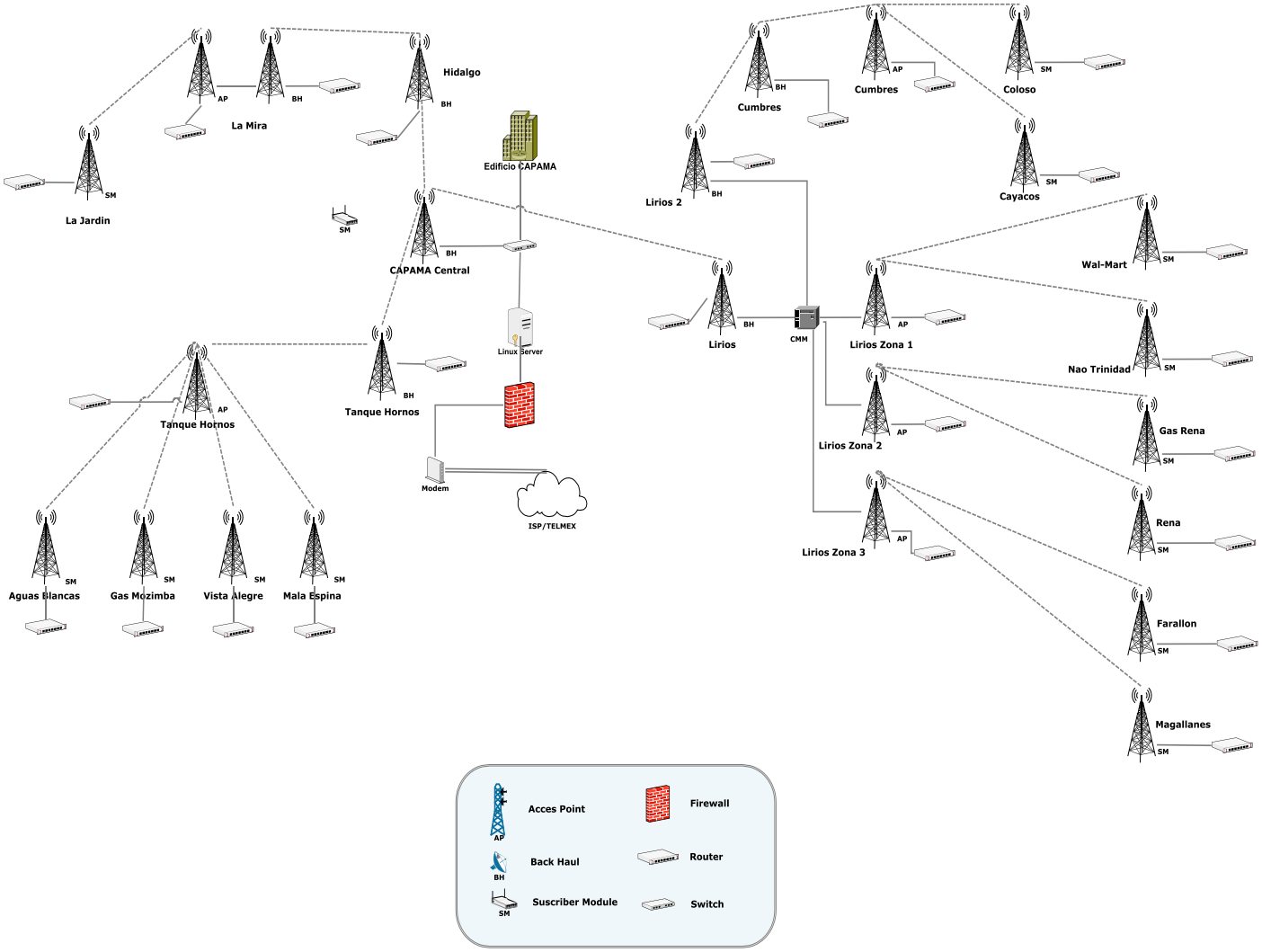

Figura 18 - Diagrama de reestructuración de red CAPAMA.

En la imagen anterior se propone la nueva red con tecnología CANOPY de MOTOROLA (Figura 18).

¿Por qué CANOPY?

Al investigar encontramos solución al problema del pago de frecuencias ya que se detectó un tipo de red en banda ancha que es confiable, económica y no debe pagarse, al menos por el usuario en uso de frecuencias, la empresa de la red lo tiene concesionado. La solución inalámbrica Canopy de Internet funciona en el espectro de Infraestructura en Información Nacional Sin Licencia (U-NII) de 5.25-5.35GHz y 5.725-5.825GHz, por lo que no hay necesidad de adquirir espectro o licencia para sitios de la empresa Motorola, los costos iníciales de la tecnología Canopy son mucho menores que con cualquier otra opción de conectividad y es tan rápida o más que las otras alternativas de dial-up por ejemplo: ISDN, DSL, MMDS, cable o satélite, también elimina la necesidad de utilizar la red telefónica o de cable existente.

Bajo dicha red se podrá explotar aplicaciones como: Extensión de LAN's, servicio de Internet, Conexiones punto-a-punto de alta velocidad, Multicast de Video, Backhaul punto-multipunto, Vigilancia por Video, Voice Over IP.

La instalación y mantenimiento de la red CANOPY es más simple que cualquier otra solución inalámbrica o de banda ancha, brinda recursos de control y diagnostico accesibles por interfaz de web, además posee múltiples capas de seguridad a través de la encriptación en la interfaz de aire, como se muestra en la siguiente imagen:

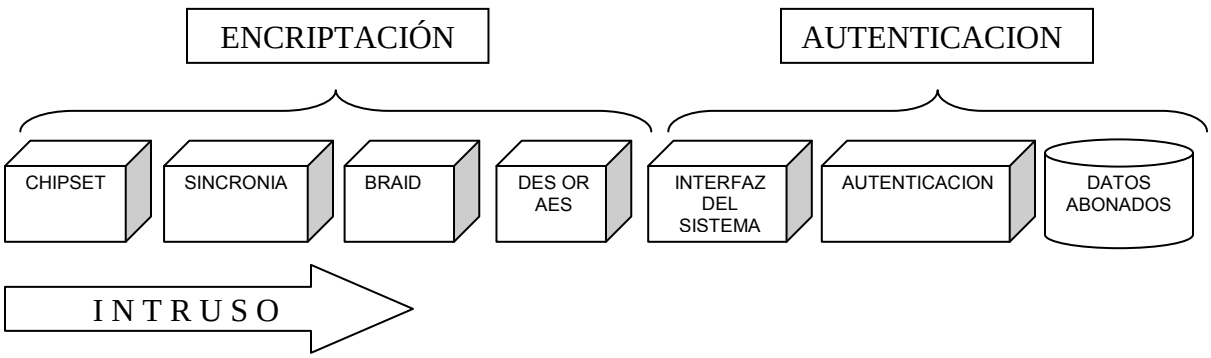

Figura 19 - Capas de seguridad de la red CANOPY.

La encriptación abarca cuatro procesos como se muestra en la (figura 19) y se define como el proceso para volver ilegible la información que se maneja dentro de la red. La autenticación es el proceso de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. Dentro de ésta existe un Software llamado Bandwidth Authentication Manager (BAM) para dos funciones básicas, primero el BAM autentica a todos los usuarios antes de permitir su acceso a la red de CANOPY y el segundo le permite variar el ancho de banda de los distintos usuarios, proporcionando una velocidad superior a otras soluciones de de banda ancha inalámbrica.

4.2 TECNOLOGÍA MOTOROLA SERIES CANOPY.

Figura 21 - Dispositivo Motorola CANOPY

La plataforma inalámbrica de banda ancha CANOPY permite convertirse en un Proveedor de Servicios de Internet de la manera más rápida y económica.

Motorola es conocida a nivel mundial por la innovación y liderazgo en comunicación inalámbrica de banda ancha. Dicha empresa es líder en comunicaciones globales y pertenece a los Fortune 100 (las 100 compañías más grandes de EEUU).

Figura 20 - Equipos de red WiFi CANOPY.

El producto: Motorola Canopy System es la solución de banda ancha que reduce significativamente el costo y el tiempo que se necesita para ofrecer un servicio inalámbrico. Los servicios que soportan son voz, video, seguridad, e Internet.

La plataforma Motorola CANOPY dispone de una conectividad robusta de alta velocidad para redes privadas como gobiernos o empresas. Esta plataforma es escalable y segura soportando aplicaciones de alta velocidad. Sus sistemas de punto-punto y punto-multipunto se han desarrollado en más de 100 países del mundo. CANOPY opera en la banda de 5GHz U-NII sin licencia, por lo que no hay necesidad de adquirir espectro o licencia para sitios. Y además, como es una plataforma inalámbrica, no existe la necesidad de utilizar la red telefónica o de cable existente.

Su diseño sencillo de red la hace muy fácil de instalar. Y con las pequeñas celdas de CANOPY, no existe la necesidad de coordinación, en modo que un sistema CANOPY de un solo sitio puede comenzar a prestar servicios rápidamente a una comunidad que se encuentre dentro de tres kilómetros. Las unidades AP Canopy incluyen todas las capacidades de autorización del usuario, administración de la red en diagnóstico que usted necesita para controlar y supervisar la red a distancia.

CANOPY se puede adoptar para satisfacer las necesidades de una amplia gama en comunidades de usuarios. La aplicación punto a multipunto puede proporcionar servicio tanto a domicilios particulares como a pequeñas empresas, o bien servir de enlace entre los datos dedicado en aplicaciones sobre pequeñas empresas.

Los protocolos inteligentes hacen que el despliegue y operación de grandes redes inalámbricas resulten sencillos y económicos. CANOPY es extensible para adecuarse a necesidades cambiantes, mayores áreas geográficas, aumento de la población y mayores volúmenes de tráfico. Además, al contar con transceptores adicionales aumenta la capacidad sin causar interferencia. El módulo suscriptor

CANOPY es pequeño y fácil de instalar en el sitio donde desee. No hace falta que el cliente instale software adicional, limitando aún más la posibilidad de que el usuario cometa errores, también no necesita usar grandes equipos que estorben.

A diferencia de las innumerables soluciones disponibles actualmente, este logra resultados sin complicaciones. Gracias a que sus velocidades de transferencia y descarga son iguales o mayores que las de cualquier otro servicio disponible hoy en día, este sistema puede ofrecer actualmente más de 6Mbps (velocidades globales de datos). Evidentemente, las velocidades de transferencia y descarga son afectadas por diversos factores, de modo que las velocidades reales pueden variar, pero el potencial en ofrecer un servicio extraordinario de Internet es factible con esta tecnología.

El Módulo de Punto al Acceso (AP) Canopy interactúa fácilmente con el equipo actual en su Red de Área Local (LAN) mediante Ethernet estándar. Los Módulos del punto de acceso y suscriptor son compactos, se pueden montar en exteriores, por lo que no es necesario tender o enterrar cables, ni tampoco instalar enlaces microondas. La solución CANOPY también ofrece un rendimiento superior, utilizando un esquema de modulación que mejora la calidad de la transmisión de datos y reduce la interferencia provocada por otros sistemas. La plataforma CANOPY de Motorola ofrece seguridad con la encriptación aérea que distorsiona los bits de datos y evita la interceptación, tal forma que la entrega de datos es altamente confiable. Esta solución inalámbrica de Internet en banda ancha más reciente de Motorola. Se ha sometido a rigurosas pruebas y actualmente presta sus servicios en todo el continente americano.

La plataforma Canopy Advantage está construida en el sistema de CANOPY, probado en muchos lugares y proporciona alto nivel de tolerancia a interferencias, escalabilidad, una señal fiable. Los usuarios de redes pueden alargar la vida de los sistemas por medio de mejoras en el software.

Los módulos son compatibles con todos los módulos en abonado de CANOPY, los módulos en gestión de grupos, los administradores de banda ancha y autenticación que estén instalados actualmente. Ningún equipo se vuelve obsoleto o necesita reparación. También en un futuro serán compatibles con el estándar Wi-Max.

4.3 INSTALACIÓN CANOPY.

El sencillo diseño de la red facilita la instalación del producto:

1. Instalar el Clúster AP Canopy. Es un sitio con seis Módulos AP incluye seis Módulos (AP) y un Módulo de Administración de Clústeres (CMM) para un máximo de seis Módulos AP y dos Módulos Backhaul, así como un receptor GPS, antena y un conmutador Ethernet integrado para una fácil conexión a la red.

2. Instalar módulos Backhaul Canopy (este si es necesario) para la señal alimentadora de red remota.

3. Instalar el módulo Suscriptor en el sitio del cliente. El módulo suscriptor incluye un sencillo adaptador de CA para uso interno y una conexión directa Ethernet con una computadora o red en el hogar.

Se debe montar cada equipo de la siguiente manera:

1) Unidad de Punto de Acceso CANOPY. El montaje de puede realizar utilizando abrazaderas para manguera de acero inoxidable u otros sujetadores equivalentes.

2) Kit de instalación de Punto de Acceso CANOPY. Se instala en una ubicación que permita el acceso a todo el servicio necesario y no a una distancia menor de 1.82 metros de las unidades de punto de acceso CANOPY

4.3.1 INTERFAZ WEB DE CONFIGURACIÓN CANOPY.

Las páginas web están disponibles para cada unidad Canopy, estas se utilizan para configurar, se puede tener acceso a las páginas web mediante la dirección IP para un protocolo Canopy. En la siguiente figura se muestran el orden de estas páginas web y abajo la descripción.

INICIO: Contiene el mensaje de bienvenida del producto.

ESTADO: Contiene información sobre la operación del producto. Esta es la pagina web establecida, despliega los parámetros que se muestran a continuación en la (tabla 5).

Tabla 5 - Parámetros de la pagina de estado.

Parámetros	Descripción
Tipo de Dispositivo.	Deberá desplegar Punto de Acceso-Modo Puntos Múltiples. Describe la configuración a la que se inició la unidad.
Versión de Software.	Despliega la versión de Software actualmente cargado a la unidad.
Versión de FPGA.	Despliega la versión de FPGA actualmente cargada a la unidad.
Dispositivo ESN.	Despliega el Número de Serie Electrónico de la unidad.
Tiempo de operación.	Despliega el tiempo que ha estado operando la unidad desde que se aplicó la energía.
Hora del Sistema.	Despliega el tiempo en el que se recibe de la unidad GPS conectada. En caso que no haya GPS, el tiempo del sistema se fija en la pagina web —Hora y Fecha”.
Ranuras ascendentes de datos.	Solo el equipo Canopy utiliza esta información.
Ranuras descendentes de datos.	Solo el equipo Canopy utiliza esta información.
Conteo SM Registrado.	Despliega el conteo actual de módulos suscriptor registrados al punto de acceso.
Interfaz Ethernet.	Despliega la configuración de la Interfaz Ethernet. Esta puede ser una base T 10 ó 100 y también dúplex medio o total.

CONFIGURACION: Sujeta información y parámetros configurables que cambian la operación del producto.

Tabla 6 – Parámetros de la pagina de configuración.

Parámetro	Descripción
Entrada de Sincronización.	Conmuta el Punto de Acceso para generar su propio pulso de sincronización de temporización para recibir un pulso de sincronización desde una fuente externa GPS. El valor predeterminado es para que la unidad genere su propio pulso de sincronización de temporización.
Portadora de Frecuencia.	Utilice esta función para establecer la frecuencia con que funcionara el Punto de Acceso.
Datos de Enlace Descendente.	Determina la división del ancho de banda total entre el limite descendente (al Modulo Suscriptor) y el limite ascendente (desde el Modulo Suscriptor). El valor predeterminado es 75%.
Porcentaje de Enlace Ascendente Alta Prioridad.	Solo el equipo Canopy utiliza esta información.
Total NumUAckSlots.	Solo el equipo Canopy utiliza esta información.
Uacks reserved high.	Solo el equipo Canopy utiliza esta información.
NumDAcksSlots.	Solo el equipo Canopy utiliza esta información.
Dacks Reserved High.	Solo el equipo Canopy utiliza esta información.
NumCtlClots.	Solo el equipo Canopy utiliza esta información.
NumCtlSlots reserved high.	Solo el equipo Canopy utiliza esta información.
Capacidad de banda ancha de Enlace Ascendente.	Determina el límite de ancho de banda ascendente, medido en Kbps, para todos los módulos suscriptor registrados al Punto de Acceso. El valor predeterminado es 9999.
Capacidad de banda ancha de Enlace Descendente.	Determina el límite de ancho de banda ascendente, medido en Kbps, para todos los módulos suscriptor registrados al Punto de Acceso. El valor predeterminado es 9999.
IP Lan.	Determina la dirección IP del Punto de acceso a través del cable Ethernet. El valor predeterminado es 169.254.1.1
Enmascaramiento de Subred Lan.	Determina el enmascaramiento de subred para el Punto de Acceso. El valor predeterminado es 255.255.0.0
Compuerta predeterminada.	Determina la compuerta predeterminada para el Punto de Acceso. El valor predeterminado es 169.254.0.0
IP Privado.	Determina la dirección IP para el enlace RF para los Módulos Suscriptor.
Enmascaramiento de	Determina el enmascaramiento de subred para el

Subred IP Privado.	enlace RF para los Módulos Suscriptor.
Código de Color.	Este parámetro determinará en qué Punto de Acceso se registrará el Módulo Suscriptor. El Punto de acceso y el Módulo Suscriptor deben tener el mismo código de color cuando se realice el registro. El rango para este parámetro es 0 a 254. El valor predeterminado es 0.
ID de Sector.	Despliega un número que se envía a todos los Módulos Suscriptor registrados. Se utiliza para identificar a qué Punto de Acceso está registrado un suscriptor. El rango para este parámetro es 0 a 15. El valor predeterminado es 0.
Rango Máximo.	Sólo el equipo Canopy utiliza esta información.
Auto-Actualización de la página web.	Determina la frecuencia con que se actualizara las páginas web automáticamente. Esta medida es en segundos. El valor predeterminado es 0, lo que nunca actualizará las páginas web.
Desplegar Sólo acceso.	Introduzca una contraseña para que el estado de las páginas sea Sólo Desplegar. El valor predeterminado es sin contraseña.
Acceso Total.	Introduzca una contraseña para permitir acceso total (ver y cambiar) a las páginas web. El valor predeterminado es no tener ningún valor.
Secuencia Ordenada de Comunidad.	Determina el acceso a la comunidad para informes de SNMP.
Subred de acceso.	Determina qué subredes pueden enviar información de SNMP.
Dirección de Captura.	Determina la dirección IP de la unidad donde se transmitirá la información de captura de SNMP.

REGISTRO DE EVENTOS: Contiene información que se registra desde el módulo suscriptor para propósitos de resolución de problemas. Se puede dar clic en el botón Limpiar Registro de Eventos, para limpiar el registro. No se debe borrar el archivo de registro, ya que se dificultará la resolución de problemas que puedan surgir.

LUID SELECCIONADO: Esta conecta a un Modulo Suscriptor registrado en el enlace RF, para ver sus páginas web internas. La pagina web Sesiones determina que LUID corresponde a un Módulo suscriptor especifico. Se introduce el LUID en el campo desplegado y después se da clic en Cambiar LUID, para establecer el parámetro. También se da clic en Ver Módem del Suscriptor Actual para tener acceso al Modulo Suscriptor con ese LUID.

PRUEBA DE ENLACE: Esta tiene una prueba para medir el rendimiento y eficiencia del enlace RF. Para esto se necesita introducir un número en el campo marcado Duración para elegir la duración de la prueba, este valor se mide en segundos. Para iniciar la prueba de enlace se da clic en el botón Iniciar Prueba, la prueba se ejecutará por la duración establecida. Si la pagina web no se establece para que se actualice automáticamente, se puede pulsar el botón Actualizar Pantalla, para que se desplieguen los resultados. Los campos clave son:

- VELOCIDAD de enlace descendente y VELOCIDAD de enlace ascendente los cuales se miden en bits por segundo.
- Eficiencia de Enlace Descendente y Eficiencia de Enlace Ascendente que se miden en porcentajes.

HORA Y FECHA: Establece la hora y fecha del sistema de la pagina web para un Punto de Acceso que no utiliza GPS.

SESIONES: Esta despliega cuáles son los módulos suscriptor que se han registrado con el Punto de Acceso, en la siguiente tabla se muestran los parámetros y sus respectivas descripciones.

Tabla 7 - Parametros de la pagina de sesiones.

Parámetro	Descripción
LUID.	Despliega la ID de la unidad lógica para el Módulo Suscriptor especifico.
MAC.	Despliega la dirección de capa 2 para el Módulo Suscriptor específico.
ESTADO.	Despliega el estado actual (desocupado o en sesión) para el Módulo Suscriptor específico.
Sesión de Tiempo Improductivo.	Sólo el equipo Canopy utiliza esta información.
Retardo de Aire.	Despliega la distancia desde el Punto de Acceso al Módulo Suscriptor específico.
Utilizado.	Sólo el equipo Canopy utiliza esta información.
Conteo de Sesión.	Despliega el número de sesiones que el Módulo Suscriptor específico ha tenido con el Punto de Acceso.
Conteo de Registro.	Sólo el equipo Canopy utiliza esta información.
Conteo de Nuevo Registro.	Sólo el equipo Canopy utiliza esta información.
SRI Promedio.	Despliega el valor RSSI promedio del Módulo Suscriptor específico.

Último RSSI.	Despliega el valor RSSI conocido del Módulo Suscriptor específico.
Fluctuación Promedio.	Despliega el valor de Fluctuación para el Módulo Suscriptor específico.
Última Fluctuación	Despliega el último valor de Fluctuación conocido del Módulo Suscriptor específico.

ESTADO GPS: Despliega información del módulo GPS ubicado en el Kit de Instalación de Punto de Acceso Canopy.

ESTADO DE PAQUETE: Despliega el rendimiento e información de error de TCP para la conexión Ethernet del Punto de Acceso.

4.3.2 ESPECIFICACIONES TÉCNICAS DEL SISTEMA CANOPY.

Características de Operación de RF:

- Margen de frecuencia: 5.25 - 5.35 GHz y 5.75 - 5.85 GHz.
- Modulación: Alto Índice de Modulación BFSK (optimizado para rechazar interferencia).
- Portadora a interferencia: 3 dB 10-4 BER@ a -65 dbm.
- Velocidad de datos: Multipunto a 10 Mbps
- 10 Mbps Backhaul.
- Margen de Funcionamiento: Hasta 3 kilómetros (2 millas) con antena integrada a 5.2GHz.
- Hasta 16 kilómetros (10 millas) con reflector pasivo en 5.7GHz.

Características Eléctricas:

- Suministro de alimentación: Alimentación por Ethernet 24 VCC a 0.3 Amp. (estado activo).
- Interfaz: Autodetección RJ45 10/100 BaseT—Dúplex medio / completo.
- Velocidad auto negociada (en conformidad con 802.3).

Aspectos ambientales:

- Temperatura de operación: -30 ºC a +55 ºC (-40 ºF a + 131 ºF).

- Humedad de operación: 100%, con condensación.
- Resistencia al viento: 190km/hora.
- Dimensiones: 29.9 cm Alto x 8.6 cm Ancho x 8.6 cm.
- Profundidad (11.75 x 3.4 x 3.4 pulg.).
- Peso: 0.5 Kg.

Hardware.

- No se requiere licencia de la FCC (Comisión Federal de Comunicaciones) para ninguno de los componentes.
- 1008CK - Módulo en Administración de Clústeres.
- Incluye antena para sincronización automática con AP Conmutador Ethernet integrado.
- Suministro de alimentación de CA para 6 unidades AP Canopy y 2 unidades BH Canopy 5200AP / 5700AP - Módulo AP Canopy.
- Medidas: 29.9 cm x 8.6 cm x 8.6 cm (11.75 x 3.4 x 3.4 pulg.).
- Conexión Ethernet 10/100baseT.

5200SM / 5700SM - Módulo SM Canopy.

- Medidas: 29.9 cm x 8.6 cm x 8.6 cm (11.75 x 3.4 x 3.4 pulg.).
- Cable único – RJ45 estándar, Ethernet de 8 clavijas.
- Adaptador sencillo de CA para uso interno Aprobado por UL (Estándares de seguridad).

5700BH – Módulo Backhaul Canopy.

- Unidad BH a 5.8 GHz, sin interferencia con enlace 5200AP a 5200SM Conexión Ethernet 10/100baseT aprobado por UL (Underwriters Laboratories).

300SS – Supresor de Sobrecargas Canopy.

- Supresor de sobrecargas opcional para conexión de cable Ethernet. Con montaje para exteriores, e incluye conexión para toma a tierra.

- 5.2 GHz: FCC ID #: ABZ89FC3789.
- 5.7 GHz: FCC ID #: ABZ89FC4816.

CONCLUSIÓN.

El presente documento, tiene el propósito de ofrecer una solución a un problema, como el de CAPAMA (Comisión de Agua Potable y Alcantarillado del Municipio de Acapulco), el implementar un sistema de red inalámbrica que sea eficiente y barato, ya que actualmente los servicios que brinda a los habitantes de esta ciudad es muy deficiente, lo que ocasiona pérdida de tiempo, pérdidas monetarias, además de no satisfacer las necesidades de dicha dependencia sobre los usuarios.

Por lo cual se deberá encontrar una solución que cuente con un sistema en redes inalámbricas de banda ancha ya que es necesario llevar un adecuado control de los servicios y mandar la información de los diferentes módulos a CAPAMA en un lapso de tiempo. La presente tesis propone una tecnología en redes inalámbricas llamada CANOPY, la cual ayudará con la mejora de la comunicación de los módulos que existen en todo el puerto de la dependencia de CAPAMA, así como mejorar los servicios que brinda a los usuarios día a día.

Se plantea la posibilidad de enviar video de las estaciones más conflictivas (vandalismo), en tiempo real a un servidor de video dedicado en la central de comunicaciones. Además es necesario ampliar la red para que se puedan captar datos de la zona Diamante y las que se encuentran en la ladera del río papagayo, para automatizar dichas estaciones además de captar datos de medición en tiempo real. Enseguida se agrega el costo aproximado de punto de acceso y accesorios en la (tabla 8).

Tabla 8 - Costo de modulos y accesorios CANOPY Motorola.

				CANT	P.U. M.N.
5.2 GHz	AP	5250APDD	5.2 GHz Advantage Access Point	1	$28,703.57
5.2 GHz	SM	5250SMDD	5.2 GHz Advantage Subscriber Module	1	$13,556.57
	ACC	27RDD	Reflector Hardware Kit	1	$1,514.70
	ACC	600SSC	Ethernet Surge Suppressor (1xcanopy)	1	$454.41
	ACC	SMMB1A	Universal Mounting Bracket	1	$378.68
	ACC	ACPSSW-09A	Power Supply 90-240 VAC, 50-60 Hz (1xcanopy)	1	$261.63

Según el estudio realizado serán necesarios otros 14 Access Point para la recolección de información.

Al aumentar la red de infraestructura existente se podrá acceder a servicios de medición en consumo de agua en tiempo real, detección de fugas, control del suministro del servicio por falta de pago, introducción del sistema de macro medición para saber la cantidad de agua que entra al puerto y cuanta se está distribuyendo, así como cuanta se está perdiendo.

Se podrá anexar el sistema de adquisición en tiempo real y control para concentrar en una sola red el sistema, incluyendo el área de automatización y control, evitando con esto los problemas de comunicación y manejo de información. También se anexará para dicha red un sistema de radios IP de corto alcance para evitar el uso de teléfonos celulares o radiocomunicación entre los distintos trabajadores en campo de CAPAMA. Se podrá vender o sub arrendar el servicio de telecomunicaciones a otras instituciones como el Municipio para la transportación de datos entre sus distintas oficinas.

En el tiempo transcurrido durante la investigación de esta investigación, se realizo la instalación de una parte en dicha red, según lo que se estudió se demuestra que es válida la hipótesis planteada en este trabajo, debido a que es factible implementar la red con tecnología CANOPY de Motorola, y no existe

ninguna duda que es la mejor opción ya que ha mejorado los servicios que brinda CAPAMA con la parte instalada de la red antes mencionada.

ANEXO 1.

- **Lista referenciada en la instalación del sistema Canopy (puerto de Acapulco).**

Tabla 9 - Puntos del sistema CANOPY.

Sitio	Equipo	Marca	Frecuencia	Frec. operación	Se comunica con:
Almacén Aguas Blancas	Suscriber Module	Motorola Canopy	5.2 Ghz	5.315 Ghz	Hornos
Malaespina	Suscriber Module	Motorola Canopy	5.2 Ghz	5.315 Ghz	Hornos
Farallón	Suscriber Module	Motorola Canopy	5.2 Ghz	5.300 Ghz	Lirios
Hidalgo	BackHaul Master	Motorola Canopy	5.7 Ghz	5.750 Ghz	Lirios
Gasolinera Ejido(Fuera operación)	Suscriber Module	Motorola Canopy	5.2 Ghz	5.315 Ghz	Hornos
Rena	Suscriber Module	Motorola Canopy Advantaje	5.2 Ghz	5.290 Ghz	Lirios
Apazco Cruces	Suscriber Module	Motorola Canopy Advantaje	5.2 Ghz	5.295 Ghz	Lirios
Lirios	BackHaul Master	Motorola Canopy	5.7 Ghz	5.740 Ghz	
Zona1 Lirios	Access Point	Motorola Canopy Advantaje	5.2 Ghz	5.325 Ghz	
Zona 2 Lirios	Access Point	Motorola Canopy	5.2 Ghz	5.290	

		Advantaje		Ghz	
Zona 3 Lirios	Access Point	Motorola Canopy Advantaje	5.2 Ghz	5.300 Ghz	
Lirios	Cluster Management module	Motorola Canopy			
Lirios 2	BackHaul Master	Motorola Canopy	5.7 Ghz	5.770 Ghz	
Gasolinera Rena	Suscriber Module	Motorola Canopy	5.2 Ghz	5.290 Ghz	Lirios
Vista Alegre	Suscriber Module	Motorola Canopy	5.2 Ghz	5.315 Ghz	Hornos
Nao Trinidad	Suscriber Module	Motorola Canopy	5.2 Ghz	5.325 Ghz	Lirios
Tanque Hornos	BackHaul Slave	Motorola Canopy	5.7 Ghz	5.770 Ghz	Hidalgo
Tanque Hornos	Access Point	Motorola Canopy	5.2 Ghz	5.315 Ghz	
Gasolinera Farallón	Suscriber Module	Motorola Canopy Advantaje	5.2 Ghz	5.300 Ghz	Lirios
Central	BackHaul Slave	Motorola Canopy	5.7 Ghz	5.740 Ghz	Hidalgo
Central	BackHaul Master	Motorola Canopy	5.7 Ghz	5.770 Ghz	
Cayaco2	Suscriber Module	Motorola Canopy	5.2 Ghz	5.275 Ghz	Cumbres
Capama-Jardín	Suscriber Module	Motorola Canopy	5.2 Ghz	5.775	La Mira

				Ghz	
Cumbres	BackHaul Slave	Motorola Canopy	5.7 Ghz	5.770 Ghz	Lirios
cumbres AP	Access Point	Motorola Canopy Advantaje	5.2 Ghz	5.275 Ghz	
Coloso	Suscriber Module	Motorola Canopy	5.2 Ghz	5.225 Ghz	Cumbres
Wallmart	Suscriber Module	Motorola Canopy	5.2 Ghz	5.325 Ghz	Lirios
La Mira	backHaul Slave	Motorola Canopy	5.7 Ghz	5.750 Ghz	Hidalgo
La Mira	Access Point	Motorola Canopy	5.7 Ghz	5.775 Ghz	Jardín

ANEXO 2.

Tabla 10 - Coordenadas geográficas de los distintos puntos de la red.

SITIO	LATITUD	LONGITUD
Pto Cementerio	16°54'45.27"N	99°49'20.76"O
Tanque Altamirano	16°53'40.73"N	99°56'40.68"O
Garza Zapata 1	16°53'46.73"N	99°49'57.31"O
Tanque La Fortaleza	16°50'10.64"N	99°54'49.60"O
Tanque La Mira	16°51'5.45"N	99°55'1.41"O
Tanque Club Deportivo	16°51'43.73"N	99°51'0.71"O
Cisterna Unidad Vte Guerrero	16°46'20.82"N	99°46'18.97"O
Tanque Miramar 2	16°48'44.50"N	99°49'29.61"O
Colosio 2	16°48'0.04"N	99°48'15.19"O
Colosio 5	16°47'40.42"N	99°47'54.05"O
Tanque Brisas	16°49'4.83"N	99°51'16.68"O
Tanque Pirámides	16°50'2.44"N	99°50'42.94"O
Tanque Cumbres de Llano Largo	16°49'46.49"N	99°50'30.20"O
Tanque Club Deportivo	16°51'40.91"N	99°50'36.54"O
Malaespina	16°51'26.74"N	99°53'47.98"O
Tanque Hornos	16°52'12.24"N	99°53'25.93"O

Desde el cuadro de oficinas centrales se comunica a los (3) repetidores por ahora y desde esta las dos redes, las de datos para captura, servicios como Internet y colector de datos en medición del agua en tiempo real para usuarios medianos y grandes, todo centralizado en CAPAMA del centro (Azueta).

En base a esto se hizo varios planos de Acapulco (Imágenes satelitales) con las distintas antenas y colectores para observar las zonas de cobertura y las necesidades de comunicación.

ANEXO 3.

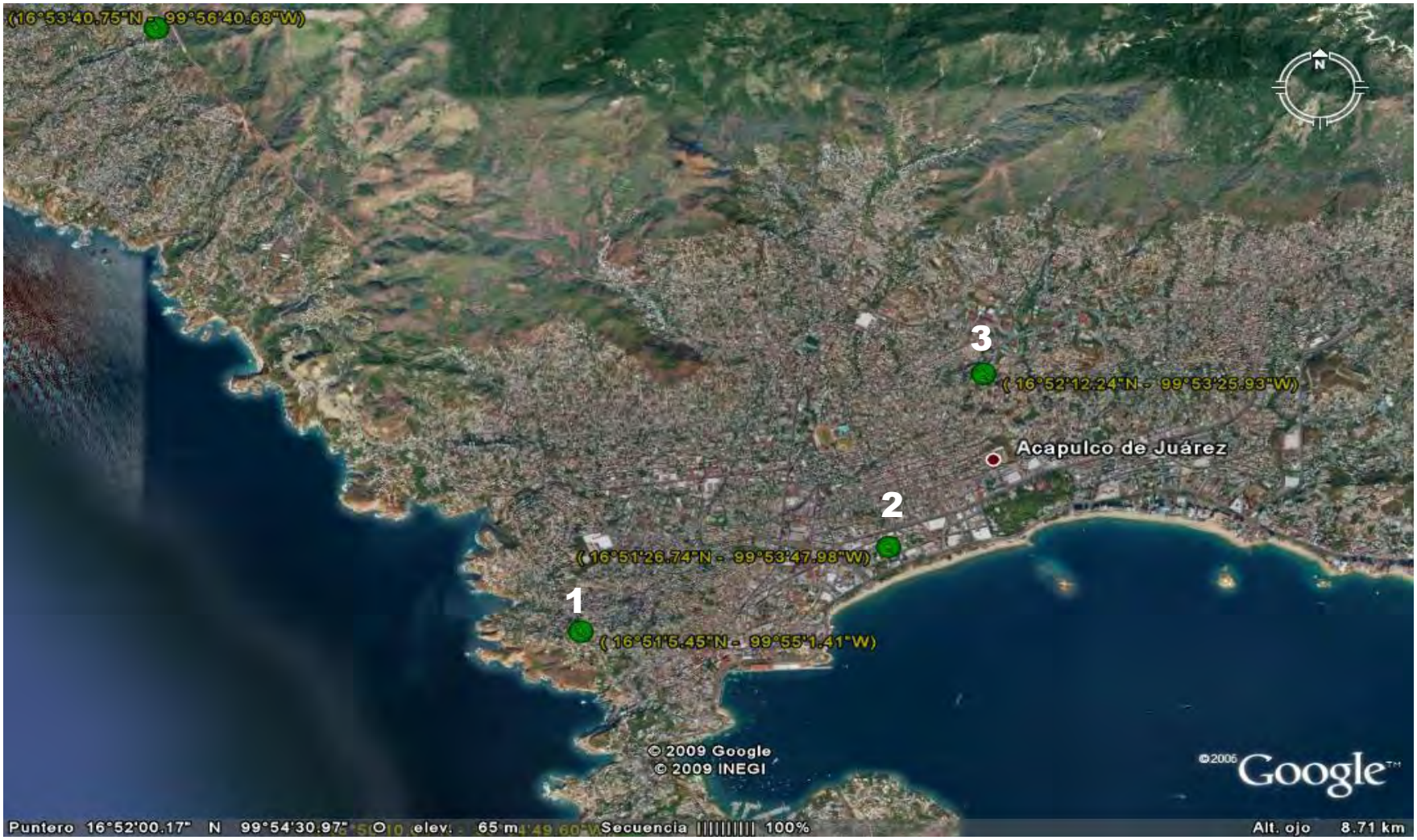

Figura 22 - Imagen satelital 1.

En la (Figura 22) se muestra las coordenadas de los tanques de La mira[1], Hornos[2] y del centro de operaciones Malaespina[3].

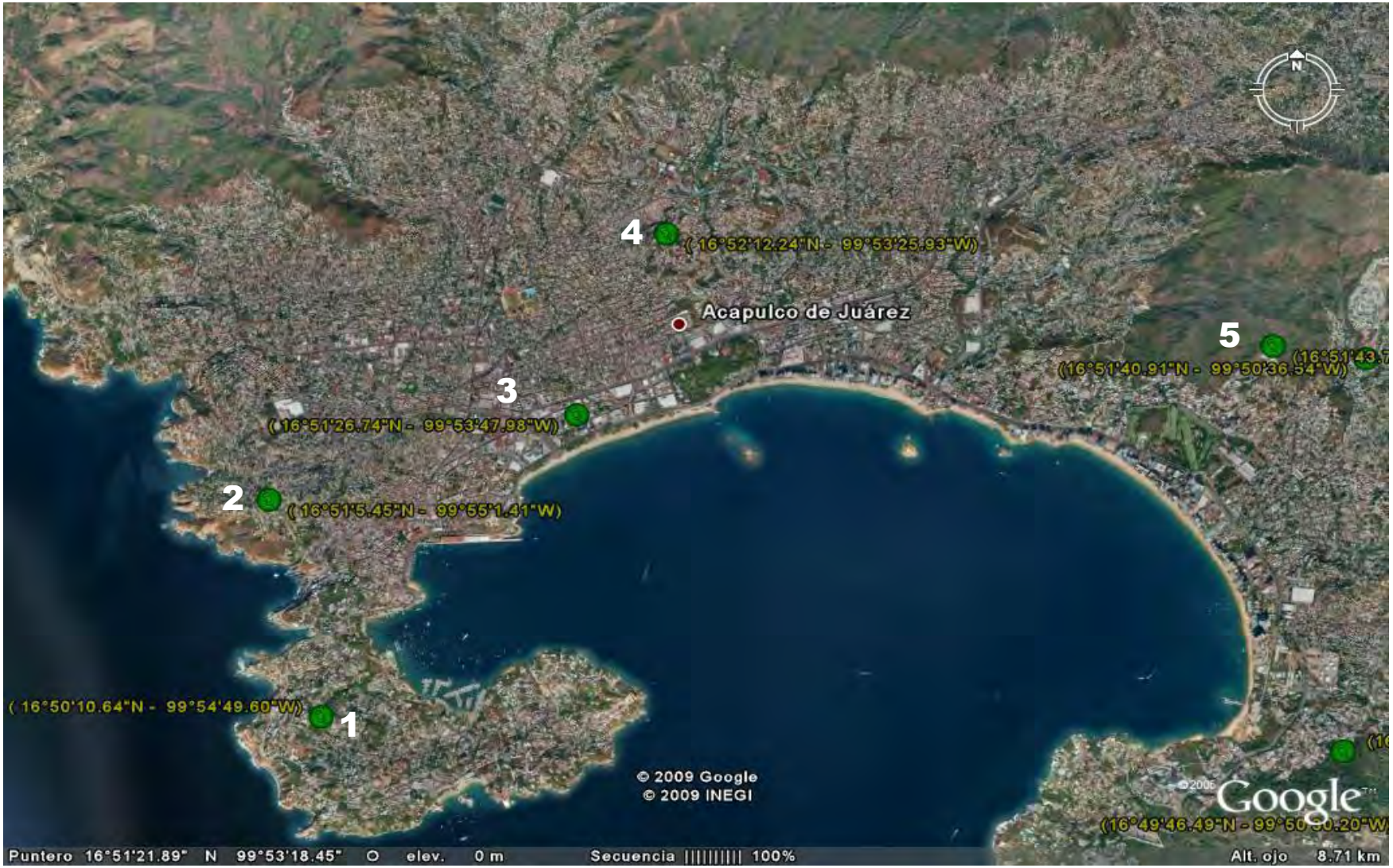

Figura 23 - Imagen satelital 2.

En la (Figura 23) se muestra las coordenadas de los tanques de: la Fortaleza[1], la Mira[2], Hornos[4], club deportivo[5] y del centro de operaciones Malaespina[3].

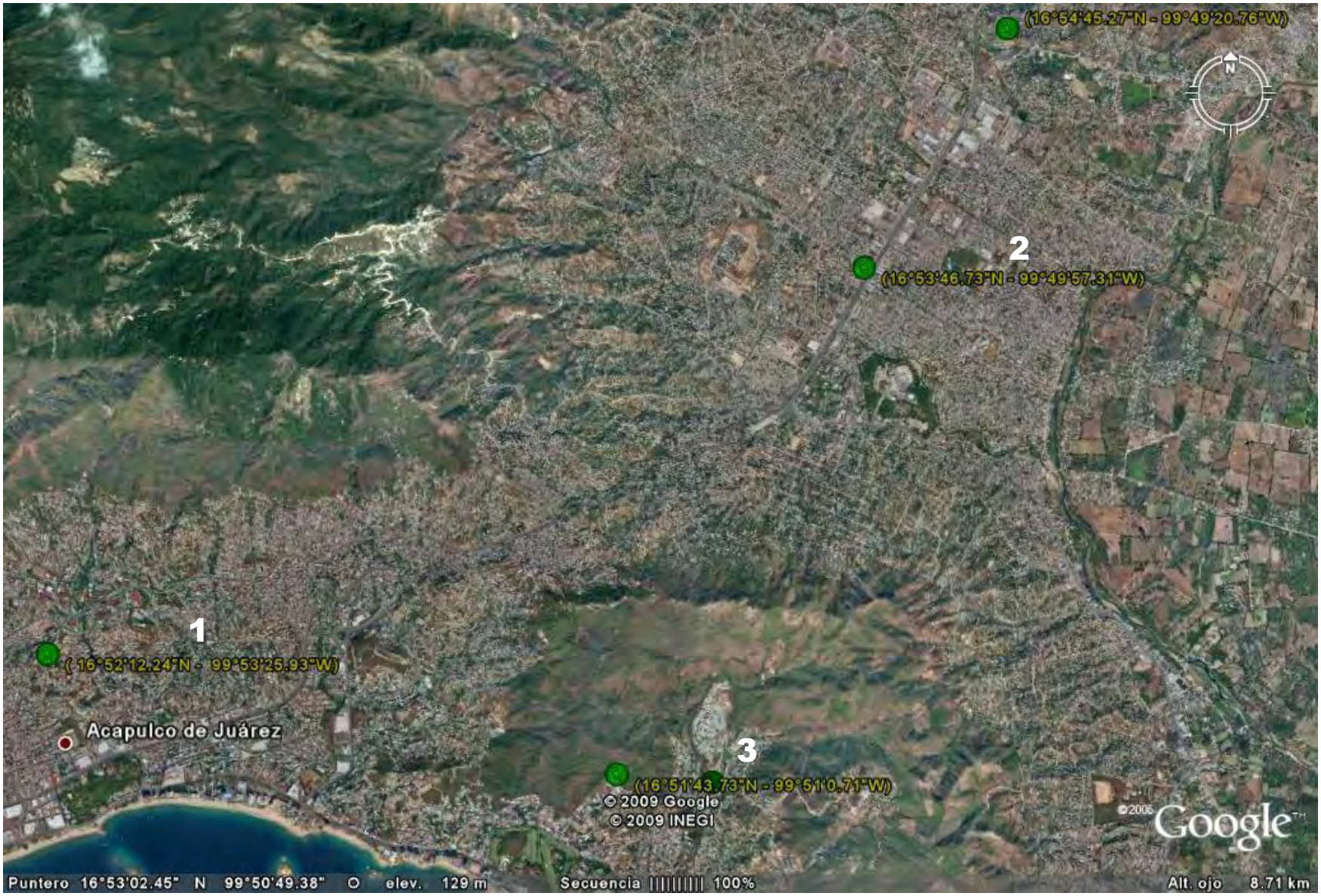

Figura 24 - Imagen satelital 3.

En la (Figura 24) se muestra las coordenadas de los tanques de: Hornos[1], club deportivo[3] y del centro de operaciónes Garza Zapata 1[2].

Figura 25 - Imagen satelital 4.

En la (Figura 25) se muestra las coordenadas de los tanques de: club deportivo[1], Piramides[2], Cumbres de llano largo[3], Brisas[4] y Miramar II[5].

Figura 26 - Imagen satelital 5.

En la (Figura 26) se muestra las coordenadas de los tanques de: Miramar II[1], Sisterna Unidad Vicente Gro[4] y centro de operaciones Colosio II[2], Colosio V[3].

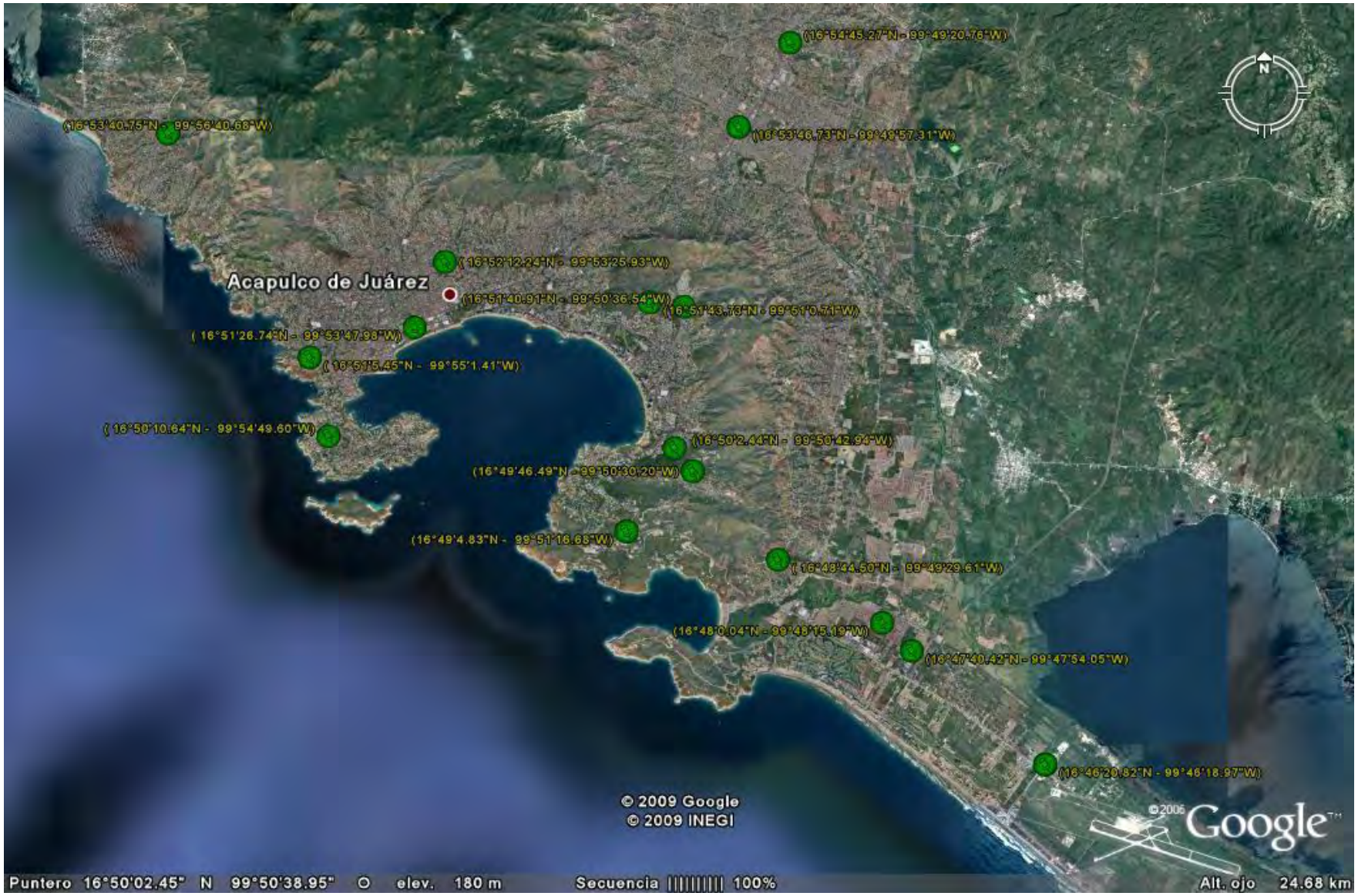

Figura 27 - Imagen satelital VI.

En la (Figura 27) se muestra todas las coordenadas de los tanques y de los centros de operación del puerto de acapulco.

ANEXO 4.

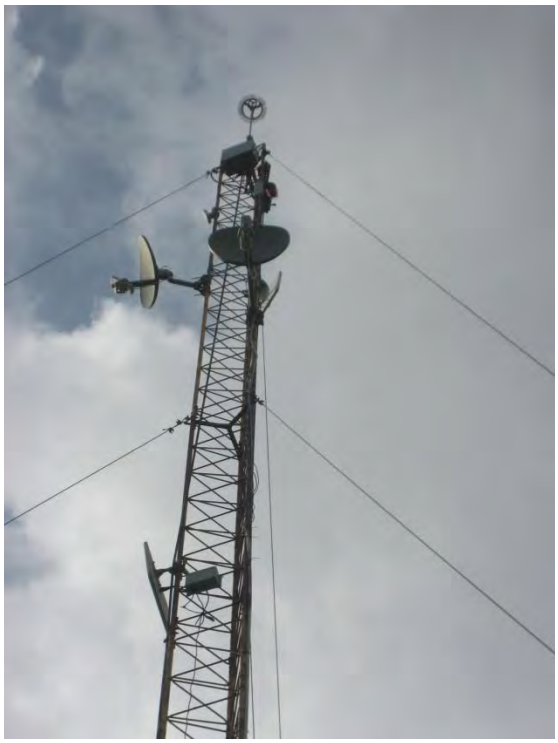

Figura 28 - Antena BH (Colonia 20 de Noviembre).

Figura 29 -Antena BH (Colonia 20 de Noviembre).

Figura 30 - Antena BH (Centro de operación: Capitán Malaespina)

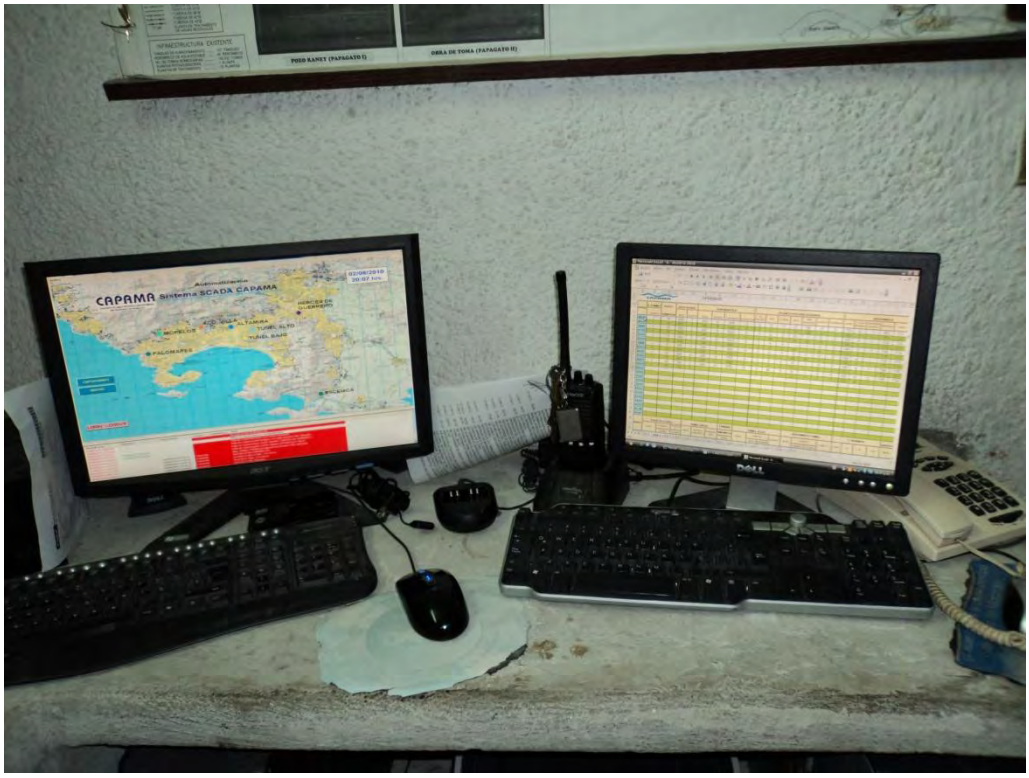

Figura 31 - Funcionamiento de la red: Monitoreo con el sistema SCADA de CAPAMA.

Figura 32 - Servidor de CAPAMA.

Figura 33- Rack en CAPAMA.

Figura 34 - Modulo de Administración de cluster.

BIBLIOGRAFÍA

- Computer Networks
  Autor: Andrew S. Tanenbaum
  Third Edition.
  Prentice Hall PTR.

- Redes Locales: Instalación y configuración básicas
  José Luís Raya, Laura Raya, Miguel A. Martínez.
  Alfaomega Ra – ma.

- Revista del Instituto Politécnico Nacional (IPN)
  CONVERSUS No. 50 y No. 62.

- Redes Globales de Información con Internet y TCP/IP.
  Douglas E. Comer
  Pearson, Tercera Edición.

- Diccionario de COMPUTACION.
  Alan Freedman
  Mc Graw Hill, Quinta edición.

- TechRepublic`s ultímate guide to Enterprise wireless LAN security
  Version 1.0 January 10, 2007
  By George Ou.

GLOSARIO.

A

Applets: Es un componente de una aplicación que se ejecuta en el contexto de otro programa. Por ejemplo, un navegador web.

Archivo: Es un conjunto de bits almacenado en un dispositivo periférico.

ArcNet: Conocido también como CamelCased, ARCnet, siglas de Attached Resource Computer NETwork) es un protocolo de la red de área local (LAN), similar en propósito a Ethernet o al token ring. ARCNET era el primer sistema extensamente disponible del establecimiento de una red para los microordenadores y llegó a ser popular en los años 80 para las tareas de la ofimática.

AES: Un reciente estándar de cifrado basado en el algoritmo Rijndael, AES ha sido aprobado por los EE.UU. Instituto Nacional de Estándares y Tecnología (NIST) de la Federal Information Processing Standard (FIPS-197). AES es un algoritmo de cifrado simétrico que serán utilizados por las organizaciones de Gobierno de los EE.UU. y de muchas otras organizaciones en el futuro, para proteger la transmisión de información sensible. AES se está incorporando en el estándar IEEE 802.11i de seguridad WLAN 802.11.

ARPANET: (Advanced Research Projects Agency NETwork) Red Avanzada de Agencias para Proyectos de Investigación. Red de conmutación de paquetes desarrollada a principios de la década de los setenta por ARPA que se considera el origen de la actual red Internet.

ARP: (Address Resolution Protocol). Protocolo de resolución de dirección. Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware. Las computadoras que llaman el ARP difunden una solicitud a la que responde la computadora objetivo.

ASCII: (American Standard Code of Information Interchange). Estándar aceptado casi mundialmente que recoge 128 caracteres, letras, números y símbolos utilizados en procesadores de textos y algunos programas de comunicaciones.

B

Backhaul: (red de retorno) conexión entre computadoras u otros equipos de telecomunicaciones encargados de hacer circular la información. Los backhaul conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación. Un backhaul es usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías alámbricas o inalámbricas.

Bluetooth: Norma internacional abierta para una tecnología de punta que posibilita la conexión inalámbrica de corto alcance de voz y datos entre computadores y portátiles, agendas digitales , teléfonos móviles, impresoras, escáneres, cámaras digitales e incluso dispositivos de casa, a través de una banda disponible a nivel global (2,4 GHz) y mundialmente compatible.

Bucle de abonado: En telecomunicaciones; También llamado El bucle local o lazo local es el cableado que se extiende entre la central telefónica (o conmutador) y las dependencias del usuario.

Bps: Bits por segundo. La velocidad de transferencia de los modems se mide en bits pos segundo.

C

CAN (Campus Area Network, Red de Area Campus)**.** Una CAN es una colección de LAN's dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilometros.

CANOPY: Es un sistema de banda ancha inalámbrica creado por Motorola y permite ampliar las redes de banda ancha de forma más rápida y con mejor relación costo-beneficio que con la tecnología con cables.

D

DAC: (Discretionary Access Control) en la seguridad de una computadora, el control de acceso discrecional (DAC) es una clase del control de acceso definida por los criterios confiados en la evaluación del sistema informático como " medios

de restringir el acceso a los objetos basados en la identidad de los temas y/o de los grupos a quienes pertenecen.

Datagramas: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información de la Internet. Los términos trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

DES: Data Encryption Standard, algoritmo de cifrado, actualmente fue sustituido por el AES.

DOS: (Disk Operating System). Programa que controla el funcionamiento del ordenador. Es el sistema operativo utilizado en la mayoría de los ordenadores personales (PCs) existentes. Aunque existen diferentes versiones del DOS, la más conocida es la desarrollada por la compañía Microsoft, denominada MS-DOS. El nombre de Sistema Operativo de Disco procede de que, en su mayor parte, el DOS permite la gestión y administración del disco duro y los disquetes.

DSL: (Digital Subscriber Line) Línea de Abonado Digital. Tecnología que permite una conexión a una red con más velocidad a través de las líneas telefónicas.

E

Ethernet: Red de área local (LAN) desarrollada por Xerox, Digital e Intel. Es el método de acceso LAN que más se utiliza (seguido por Token Ring). Ethernet es una LAN de medios compartidos. Todos los mensajes se diseminan a todos los nodos en el segmento de red. Ethernet conecta hasta 1,024 nodos a 10 Mbits por segundo sobre un par trenzado, un cable coaxial y una fibra óptica.

F

Fotodetector: La definición básica de un fotodetector radica en su funcionamiento como transductor de luz que proporciona una señal eléctrica como respuesta a la radiación óptica que incide sobre la superficie sensora.

FTP: (File Transfer Protocol) Nombre del protocolo estándar de transferencia de ficheros. Su misión es permitir a los usuarios recibir y enviar ficheros de todas las máquinas que sean servidores FTP. El usuario debe disponer del software que permita hacer la transferencia (actualmente todos los navegadores, ya disponen de ese software para recibir ficheros).

G

Gateways: (puerta de enlace). Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

H

Hardware: Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman una computadora, incluidos sus periféricos.

Home RF: Es un estándar europeo y se basa en el Teléfono inalámbrico digital mejorado (Digital Enhaced Cordless Telephone, DECT) que es un equivalente al estándar de los teléfonos celulares GSM. Transporta voz y datos por separado, al contrario que protocolos como el WiFi que transporta la voz como una forma de datos.

I

ICMP: (Internet Control Message Protocol). Protocolo de control de mensajes de interred. Protocolo usado por el IP para informar de errores y excepciones. El ICMP también incluye mensajes informativos usados por algunos programas como ping.

IEC: (International Electrotechnical Commission). Comisión Electrotécnica Internacional. Grupo industrial que escribe y distribuye estándares para productos y componentes eléctricos.

IEEE: (Institute of Electrical and Electronics Engineers). Asociación de profesionales norteamericanos que aporta criterios de estandarización de dispositivos eléctricos y electrónicos.

Impedancia: Resistencia aparente de un circuito eléctrico al paso de la corriente alterna

Infinitum: Servicio brindado por la empresa TELMEX el cual ofrece una conexión a Internet de Banda Ancha con la que puedes hablar y navegar al mismo tiempo a alta velocidad.

Interfaz: 1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características en común de interconexión física, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI. Interfaz abierta de enlace de datos.

IP: Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientada a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, seguridad, fragmentación y reensamblaje.

ISO: (International Organization for Standardization). Bajo los auspicios de la ONU, esta organización fija estándares de todo tipo que deben seguir los países miembros.

K

Kerberos: Es un protocolo de autentificación de redes que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar ataques de replay.

L

Linux: sistema operativo gratuito para computadoras personales derivado de Unix.

M

MAC O MACINTOSH: Computadora que Apple empezó a fabricar en 1984. Fue la primera computadora personal que incorporó una interfaz gráfica, con el propósito de facilitar un uso más intuitivo de la máquina. Tiene su propio sistema operativo, llamado Mac OS. El uso de la Macintosh está muy difundido entre diseñadores gráficos, artistas visuales y músicos.

Microsoft: (Microsoft Corporation, Redmond, WA) Compañía de software más grande del mundo. Microsoft fue fundada en 1975 por Paul Allen y Bill Gates, dos estudiantes universitarios que escribieron el primer intérprete BASIC para el microprocesador 8080 de Intel. Aunque también se conoce por sus lenguajes de programación y aplicaciones para computadores personales, el éxito sobresaliente de Microsoft se debe a sus sistemas operativos DOS y Windows.

Multiplexar: Técnica que permite transmitir diferentes comunicaciones a través de un único canal.

N

NetBIOS: Sistema básico de entrada/salida de red. Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y terminación de sesión, y transferencia de información.

NetBEUI: Es el protocolo utilizado por las antiguas redes basadas en Microsoft LAN Manager. Es muy rápido en pequeñas redes que no lleguen a la decena de equipos y que no muevan ficheros de gran tamaño, a partir de ahí es mejor que te decantes por otra opción y lo desinstales de tus clientes y tus servidores, esto último siempre que no tengas ningún equipo que utilice LAN Manager.

NLOS: Non Line of Sight o Fuera de la Línea de Visión, es un término utilizado en comunicaciones mediante radiofrecuencia. Se usa para describir un trayecto

parcialmente obstruido entre la ubicación del transmisor de la señal y la ubicación del receptor de la misma. Los obstáculos incluyen árboles, edificios, montañas y otras estructuras u objetos construidos por el hombre u obra de la naturaleza.

O

Onda electromagnética: es la forma de propagación de la radiación electromagnética a través del espacio, y sus aspectos teóricos están relacionados con la solución en forma de onda que admiten las ecuaciones de Maxwell. A diferencia de las ondas mecánicas, las ondas electromagnéticas no necesitan de un medio material para propagarse; es decir, pueden desplazarse por el vacío.

OS/2: Son las siglas de "Sistema operativo de segunda generación". La idea de OS/2 surgió entre IBM y Microsoft a mediados de los 80, en un intento de hacer un sucesor de MS-DOS, el cual ya empezaba a acusar el paso del tiempo y resultaba claramente desaprovechador de los recursos de las máquinas de la época (basadas en el Intel 286).

OSI: Acrónimo de Open System Interconnection (interconexión de sistemas abiertos). Es una familia de protocolos, realizados por la comisión de la OSI, que debería ser el estándar internacional de la arquitectura de las redes de sistemas de elaboración.

P

PDA: Personal Digital Assistan. Asistente Personal Digital. Programa que se encarga de atender a un usuario concreto en tareas como búsquedas de información o selecciones atendiendo a criterios personales del mismo. Suele tener tecnología de IA (Inteligencia Artificial).

POE (Power over Ethernet): (Energía sobre red). Es el medio de transmisión eléctrica sobre cable de red (RJ45) de categoría 5.

R

Radiofrecuencia: También denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre

unos 3 Hz y unos 300 GHz. El Hertz es la unidad de medida de la frecuencia de las ondas radioeléctricas, y corresponde a un ciclo por segundo.

RARP: Protocolo de Resolución de Dirección de Retorno. Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

RJ45: Es una Interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). *RJ* es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

S

Software: Término general que designa los diversos tipos de programas usados en computación.

SPX Sequenced Packet Exchange: Intercambio de Paquetes Secuencial. Protocolo confiable, orientado a conexión, que complementa el servicio de datagramas suministrado por los protocolos de capa de red (Capa 3). Novell derivó este protocolo de transporte NetWare de uso común del SPP del conjunto de protocolos XNS.

STP: (Shielded Twisted Pair). Par Trenzado Blindado. Medio de cableado de dos pares que se usa en diversas implementaciones de red. El cableado STP posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

SNMP: (Simple Network Management Protocol) Protocolo de transferencia para las direcciones IP asignadas por el servidor, servidor para el tratamiento de las direcciones IP manejadas en un sistema de información. Utilizado para obtener estadísticas de consumo de recursos de la red y servidores.

SSH: (Secure SHell). Protocolo seguro y un conjunto de herramientas para reemplazar otras más comunes (inseguras). Fue diseñado desde el principio para ofrecer un máximo de seguridad y permitir el acceso remoto a servidores de forma segura.

T

Token Ring: Red de topología de anillo que se sirve del pase de fichas para el control de acceso. La frase también se aplica a una topología de pase de fichas específica definida por IBM Corporation.

trama de datos: Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado y a la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. Los términos datagrama, mensaje, paquetey segmento también se utilizan para describir las agrupaciones de información lógica en las distintas capas del modelo de referencia OSI y en distintos círculos de tecnología.

U

Unix: Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas mas conocidos como MS-DOS están basadas en este sistema muy extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

U-NII (Unlicensed National Information Infrastructure): La Infraestructura de la Información Nacional sin Licencia es un conjunto de frecuencias de radio que se asignan para su utilización por los usuarios sin licencia de equipo de comunicaciones inalámbricas, incluyendo LAN inalámbrica 802.11a y HIPERLAN. El internacionalmente reconocido UNII banda es en realidad dividida en tres rangos de frecuencia: 5.15GHz - 5.25GHz, 5.25GHz - 5.35GHz, y 5.725GHz - 5.825GHz.

V

VPN: (Virtual Private Network) Red privada virtual. Red de comunicaciones de área ancha provista por una portadora común que suministra aquello que asemeja líneas dedicadas cuando se utilizan, pero las troncales de base se comparten

entre todos los clientes como en una red pública. Permite configurar una red privada dentro de una red pública.

W

Windows: Es el nombre del popular entorno (no es un sistema operativo y no es una aplicación) software creado por Microsoft. Su novedad es el uso de diferentes pantallas que se superponen, denominadas ventanas, para mostrar distintos tipos de información. Su implantación ha representado un gran avance en la facilidad de operación para los usuarios de ordenadores personales. Numerosos programas pueden gestionarse a través de este entorno que, además, incorpora sus propias aplicaciones como son Write y Paintbrush, entre otras.

Windows Server 2003: Windows Server 2003 es la versión de Windows para servidores lanzada por Microsoft en el año 2003. Está basada en el núcleo de Windows XP, al que se le han añadido una serie de servicios, y se le han bloqueado algunas características (para mejorar el rendimiento, o simplemente porque no serán usadas). En términos generales, Windows Server 2003 es un Windows XP simplificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor.

Wi-Fi: (Wireless Fidelity) La expresión Wi-Fi se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes de trabajo sin cables (conocidas como WLAN, Wireless Local Area Netwoks).

X

XNS: Sistema de red de Xerox. Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte principal.