UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA

F.A.F.I.

ESCUELA DE SISTEMAS

TESIS DE GRADO PREVIA A LA OBTENCION DEL TITULO

DE INGENIERO EN SISTEMAS

TEMA:

ANALISIS Y DISEÑO DE UNA RED HIBRIDA PARA LA GESTION DE VENTAS DE LA EMPRESA MORA E HIJOS DE LA CIUDAD DE BABAHOYO

AUTOR:

Freddy Ramiro Almeida Mastian

BABAHOYO - ECUADOR

2012

DEDICATORIA

El presente trabajo lo dedico con mucho cariño y esfuerzo A Mi Padre Sr. Nelson Almeida, a mi madre Sra. María Mastian símbolo de bondad y abnegación, quienes con entero sacrificio supieron entregar todo de sí, para hacer de mí un ser útil a la Patria y a la sociedad y así poder obtenerme anhelado título.

AGRADECIMIENTO

Mi profundo agradecimiento a DIOS, por la vida con cuyo consentimiento he culminado con éxito mis estudios superiores.

A mis padres por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr los objetivos.

A mis hermanos y familiares cercanos por la comprensión y apoyo moral demostrado en todo este tiempo.

A la Universidad Tècnica de Babahoyo, por medio de sus docentes ha sido el alma mater del conocimiento que nutrió el alma y mente de conocimiento valioso para la vida.

Al Ing. Freddy Jordàn Cordones, tutor, guía, y amigo por su soporte académico y constante apoyo para el desarrollo del presente trabajo.

Y a todas las personas que aunque no las nombro saben que están presentes en estas palabras por su apoyo y empuje hacia la finalización de mi carrera.

CAPITULO I

EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA.

Las computadoras hoy en día han transformado el mundo de los negocios ya que se consideran esenciales para enfrentar el reto de la globalización, actualmente los negocios deben de producir bienes y servicios de alta calidad a bajo costo y sin las computadoras, esto sería prácticamente imposible, debido a que nos proporcionan la información precisa y actual que se requiere para tomar las decisiones correctas.

El gran desarrollo alcanzado por las organizaciones en la actualidad, demanda una enorme cantidad de información. Por otro lado las empresas de nuestros días están obligadas a tomar decisiones cada vez más precisas y con mayor rapidez. La informática enfrenta estos problemas y los relaciona, estudiando la mejor forma de proporcionar la información necesaria, a fin de tomar decisiones.

Para lograr sus metas, la informática estudia el diseño y la utilización de equipo, sistemas y procedimientos que permiten captar y tratar los datos adecuados para obtener información útil en la toma de decisiones.

En la ciudad de Babahoyo se encuentra localizada la empresa MORA & HIJOS, la cual se dedica a la fabricación y venta de plantas de caucho para calzado, su almacén principal se halla ubicado en la calle Pedro Carbo entre 10 de Agosto y 5

de Junio, mientras que la sucursal está localizada en las calles General Barona entre Rocafuerte y Eloy Álvaro.

Por otro lado la fábrica de producción de plantas se encuentra en la ciudadela Barrio Lindo sector la Maternidad. La sección administrativa de la empresa se halla en los altos del almacén principal. De las visitas realizadas a la empresa se ha podido observar las siguientes deficiencias:

- No hay comunicación directa entre los puntos de venta y la fabrica.
- No se dispone de información real sobre las ventas realizadas.
- No se dispone de la información actualizada sobre las existencias en bodega o en producción para poder realizar las ventas respectivas.
- El sector administrativo no posee un acceso permanente al Internet.
- En muchas ocasiones la información es transportada en papel o en CD desde la sucursal a la matriz siendo durante el trayecto extraviada o deteriorada.

1.1.1 Formulación del Problema.

¿Cómo mejorar la gestión de ventas en la empresa Mora & hijos?

1.1.2 Delimitación del problema

Nuestro objeto de estudio es la **Ingeniería en Sistemas**

El **campo de acción** está definido en las redes y la comunicación de datos

Se trabajará con la información pertinente al año 2010.

1.2. OBJETIVOS

1.2.1 General.

Diseñar una red hibrida mediante la cual se pueda mejorar la gestión de ventas en la empresa productora de plantas de caucho Mora & hijos.

1.2.2 Específicos

- Realizar una investigación bibliográfica sobre sistemas de comunicación, redes inalámbricas, redes man y gestión de ventas.

- Llevar a cabo una investigación de campo mediante la cual se evalué la incidencia de las comunicaciones en la gestión de ventas de la empresa Mora.

- Diseñar la red hibrida, la cual constará de antenas de baja potencia, Access point y cableado estructurado.

1.3 JUSTIFICACIÓN

De lo descrito anteriormente se puede apreciar que la empresa tiene un problema en lo referente a la comunicación de datos entre las diferentes dependencias, claro que muchas veces esas dificultades son sorteadas en base a llamadas telefónicas o rápidos desplazamientos de los empleados, pero muchas veces se han perdido ventas debido a que no se conoce exactamente la existencia en bodegas de los almacenes o de la fabrica.

Si la empresa dispusiera de un sistema de comunicación de datos fácil y rápidamente podría obtener esa comunicación, seguramente no se perderían ventas y también se podría canalizar mejor la producción ya que se dispondría de información concreta sobre qué productos existen y cuáles deben ser producidos inmediatamente. De lo expuesto es claro concluir que al existir una comunicación de datos mediante una red hibrida se mejoraría notablemente la gestión de ventas de la empresa para con ello producir un bienestar empresarial y del personal que labora en la misma.

CAPITULO II

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS.

Cabe mencionar que existen muchos sistemas de comunicación dentro del ámbito informático, las redes de han constituido en el principal medio de comunicación de datos entre computadores, dentro de ellos la comunicación inalámbrica es la que actualmente a cobrado un impulso tremendo debido al avance tecnológico y al descenso de precios en los equipos de enlace.

En cuanto a tesis desarrolladas similares a la propuesta podemos mencionar que existen muy pocas, la gran mayoría de las existentes hacen referencia a redes Lan con cableado estructurado, las más recientes han sido complementadas con enlaces inalámbricos mediante access point, quizás las que pueden ser mencionadas como antecedentes son dos: La tesis del Ing. Carlos Cepeda (Ambato, Octubre 2006) y la Tesis de la Ing. Jasleide Benavides (Santo Domingo, Marzo 2006), las cuales han enlazada intranet mediante antenas con alcances entre 2 y 15 Km.)

2.2 FUNDAMENTACIÓN CIENTÍFICA

La presente tesis se fundamenta científicamente en los siguientes temas:

2.2.1 Redes

Una red es un conjunto de computadoras y/o un conjunto de dispositivos de computación enlazados entre sí para cumplir determinados objetivos como son:

- Transferencia de datos
- Compartir recursos
- Compartir procesador central
- Permitir la duplicidad de la información para tener mayor seguridad.

Esto hace posible la transmisión de información entre diferentes estaciones, accesar bases de datos o terminales remotos, ejecutar funciones en máquinas más potentes y compartir dispositivos como impresoras, fax, digitalizadores, etc.

Para la implementación de una red se emplean, entre otros, dispositivos de computación, tarjeta de interfaz de red, sistemas de cables, concentradores y software de red. Dentro de los dispositivos de computación se encuentran: las computadoras personales, estaciones de trabajo, disco duro, impresora, enruteadores. La interfaz de red ejecuta las funciones de hardware que requiere el dispositivo de computación. Los sistemas de cables son los que permiten enlazar los distintos dispositivos que forman la red. Los concentradores permiten que varias redes se conecten a través de un mismo punto y los software de red son los que manejan las funciones de alto nivel empleadas por los usuarios.

2.2.2 Topología de Redes

- Topología de Bus
- Topología de Anillo
- Topología de Anillo Doble
- Topología de Estrella
- Topología de Estrella Extendida
- Topología de Árbol
- Topología de Malla completa
-

2.2.2.1 Topología de Bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

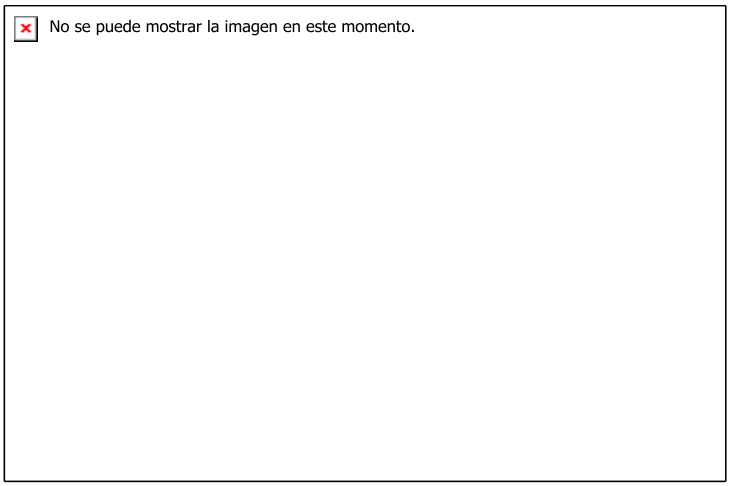


Grafico: 1 Topología de bus

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes.

Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

2.2.2.2 Topología de Anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

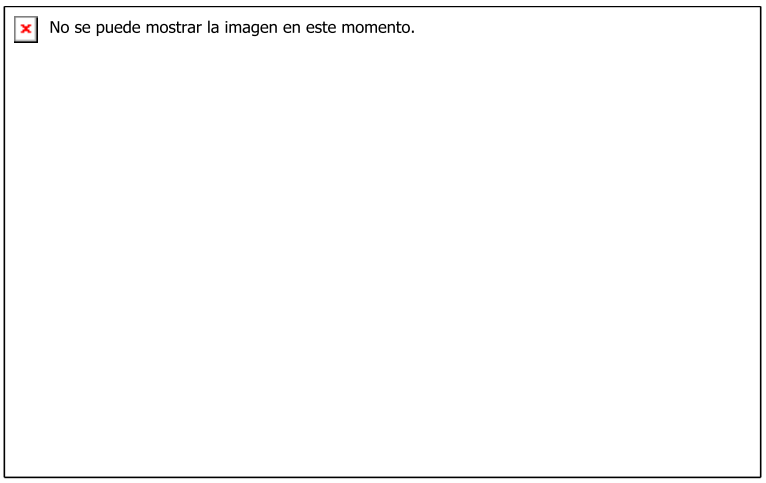


Grafico: 2 Topología de anillo

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

2.2.2.3 Topología de Anillo Doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos.

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

2.2.2.4 Topología de Estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.

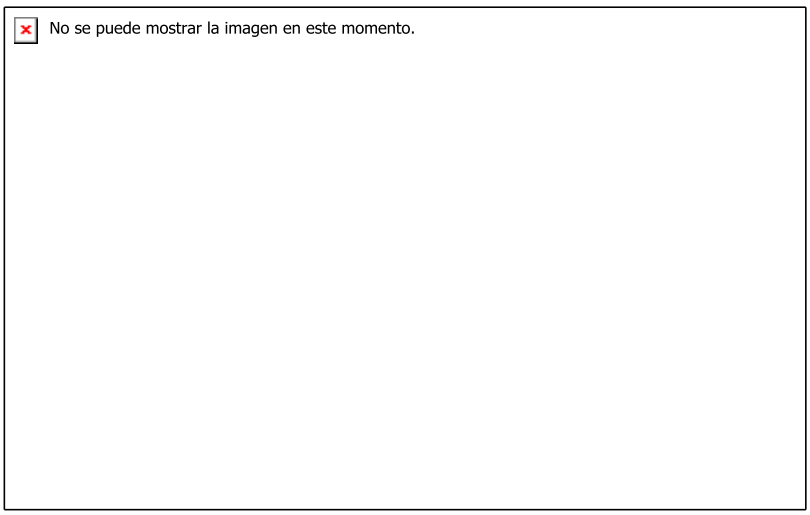


Grafico: 3 Topología en estrella

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

2.2.2.5 Topología de Estrella Extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.
La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

2.2.2.6Topología de Árbol

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

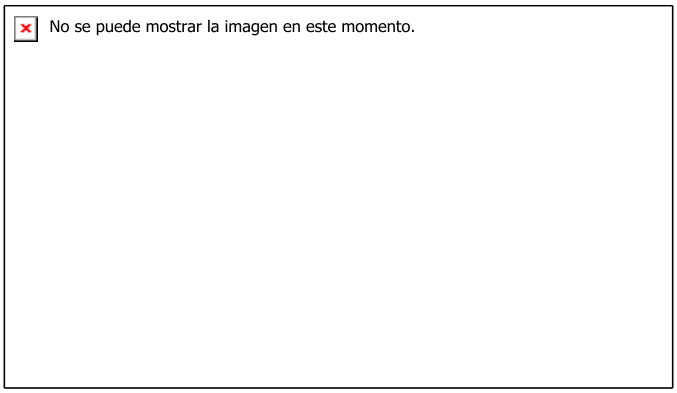


Grafico: 4 Topología en árbol

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

2.2.27. Topología de Malla Completa

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

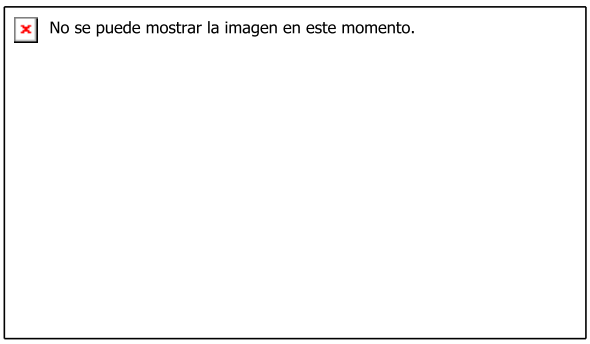


Grafico: 5 Topología en malla completa

2.2.3 Componentes de una Red

Actualmente existen muchos dispositivos que conforman una red de computadoras. Algunos de estos componentes pertenecen a la parte de hardware y otros a la parte de software. Estos son:

- Sistema de cableado
- Dispositivos de conectividad
- Dispositivos de interconexión de redes
- Sistema Operativo de Red
- Herramientas de Administración de Red

Dispositivos de Conectividad e Interconexión.

- **A** nivel físico: Concentradores o Hubs.
- A nivel de enlace: Bridges o Switches
- A nivel de Red: Routers
- A nivel de transporte: Gateways de Transporte
- A nivel de Aplicación: Gateways de Aplicación

2.2.4 Redes Ethernet

Ethernet es una especificación de red de área local (LAN) desarrollada en 1976 por Xerox, en cooperación con DEC e Intel, originalmente para conectar los miniordenadores. Se trata de una red muy difundida, de la cual se derivó la norma (o estándar) IEEE 802.3 para redes de conexión.

Ethernet utiliza un medio de difusión de bus y se basa en el método de acceso conocido como CSMA/CD para regular el tráfico en la línea de comunicación principal. Los nodos de la red están conectados por tarjetas de red unidas mediante cable coaxial (en sus dos variedades, grueso y fino), por cable con clavija tipo RJ-45, similar en apariencia al cable telefónico, y las más avanzadas mediante fibra óptica. El cableado Ethernet coaxial fino tiene un diámetro de 5 mm y puede conectar estaciones de red en una distancia de 300 m; el cableado Ethernet coaxial grueso tiene 1 cm de diámetro y puede conectar redes distantes entre sí hasta 1.000 metros.

La información en la red Ethernet se envía en tramas de longitud variable que contienen la información de control y hasta 1.500 bytes de datos. El estándar Ethernet original permite la transmisión en banda base a 10 Mbps (megabits por segundo); las tarjetas se denominan comúnmente 10BaseT, 10Base2..., según el tipo de cable de conexión. Estándares más modernos, con un cableado mejorado y con tarjetas con buses de conexión avanzados (por ejemplo, con bus PCI en vez del original ISA), permiten llegar hasta los 100 Mbps; se trata del estándar IEEE

802.3u, y las tarjetas utilizadas se denominan comúnmente 100BaseT o 10/100 (Fast Ethernet).

Más recientemente, se han presentado las denominadas Gigabit Ethernet, que alcanzan velocidades de hasta 1 gigabit por segundo (1 gigabit equivale a 1.024 megabits); se trata del estándar IEEE 802.3z.

2.2.5 Arquitectura de Redes

Para lograr que una amplia gama de dispositivos, sean enlazados para formar una red se necesita que exista compatibilidad de hardware y software o que existan interfaces complejas para permitir el éxito de la comunicación. Para facilitar dicha compatibilidad se desarrolló la arquitectura de red, la cual permitió la implementación de redes complejas con una gran variedad de equipos.

Una arquitectura de red es un plan que establece las reglas que gobiernan el diseño y la operación del hardware y el software de los componentes usados, para formar la red de computadoras. Además definen los protocolos de comunicación que gobiernan la forma en que ocurrirá la comunicación.

En las redes de computadoras modernas, las funciones de transmisión de datos son ejecutadas mediante un hardware complejo y el software de los dispositivos de la red. Para manipular esta complejidad, las funciones del software se dividen

en niveles funcionales independientes, los cuales deben cumplir los siguientes requisitos:

1) Deben ser creados donde haga falta un nivel de abstracción diferente.
2) Cada nivel debe realizar una función bien definida.
3) Sus funciones deben escogerse teniendo en cuenta la existencia de protocolos estandarizados mundialmente.
4) Las fronteras entre los niveles deben seleccionarse de manera que se minimice el flujo de información a través de las interfaces.
5) El número de niveles debe ser lo suficientemente grande como para que funciones muy distintas no coexistan en un mismo nivel, a su vez el número de niveles debe ser lo suficientemente pequeño para que la arquitectura no se vuelva inmanejable

El nivel más alto soporta a los programas de aplicación que utilizan los usuarios finales; el más bajo, maneja todos los detalles físicos concernientes a la comunicación de la red. Los softwares de comunicación se conforman siguiendo una arquitectura de red en particular y emplean un conjunto específico de protocolos de comunicación. Hoy en día existen diferentes arquitecturas de redes y sistemas de protocolos de comunicación usados en las redes de computadoras entre los que se encuentran: TCP/IP, Novell Net Ware (IPX/SPX), Apple Talk, DECnet Fase IV, Sistemas de Trabajo en Redes Xerox (XNS), SNA. La siguiente figura muestra el modelo de arquitectura de redes.

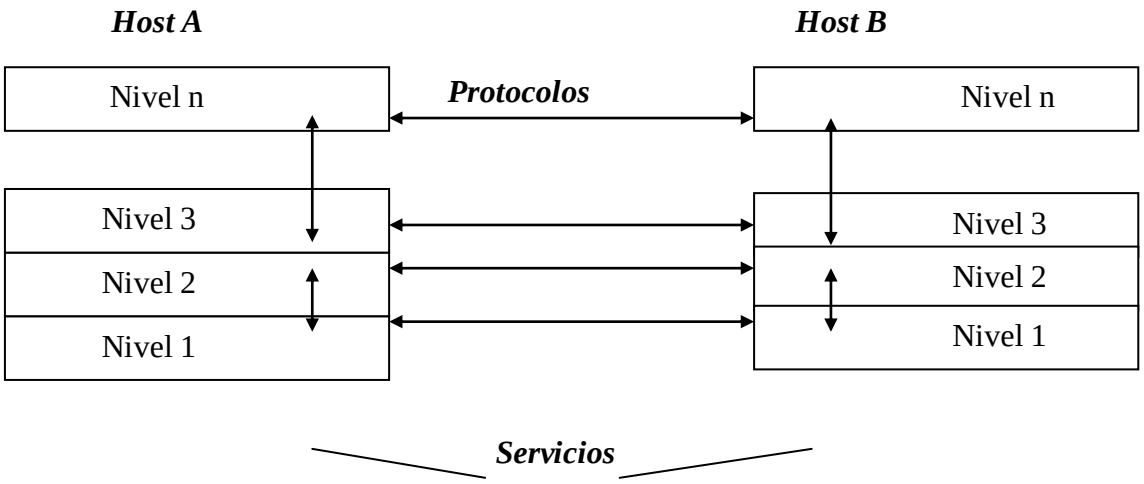


Tabla 1 Arquitectura de redes

2.2.5.1 .Modelo de Arquitectura de Redes

El modelo de arquitectura de redes está formado por *N* niveles funcionales entre los que existe una interfaz; cada nivel le proporciona un conjunto de servicios a su inmediato superior. Estos servicios se representan mediante flechas verticales. La comunicación entre capas homólogas, o sea las que pertenecen a un mismo nivel, puede realizarse de forma real o de forma virtual. La comunicación real solo ocurre en el nivel más bajo.

En el resto de los niveles ocurre la comunicación virtual. Cuando se dice que una capa de nivel n conversa con su homóloga, lo que ocurre realmente es que esta capa intercambia información a través de las interfaces que están por debajo de ella hasta el nivel inferior que es quien en realidad transfiere la información hacia su nivel homólogo; a partir de este hacia arriba serán intercambiadas las

informaciones correspondientes hasta llegar a la capa del mismo nivel. En esto consiste la comunicación virtual. Los protocolos, indicados con flechas horizontales, son usados para proporcionar los servicios entre los niveles homólogos de diferentes sistemas.

Estos definen el formato de la unidad de datos que se intercambiará y rigen la forma en la que ocurrirá la transferencia de información.

2.2.6 Protocolos de Comunicación

Los protocolos de comunicación son los estándares que especifican cómo son representados los datos al ser transferidos de una máquina a otra, cómo ocurre la transferencia, cómo se detectan los errores y cómo se envían las señales de reconocimiento. Para simplificar el diseño de protocolos y su implementación, los problemas de comunicación se separan en subproblemas que pueden resolverse independientemente. Cada subproblema es asignado a un protocolo y se corresponde con una capa de la arquitectura de redes. Generalmente los protocolos de comunicación reciben el mismo nombre de la capa a la que son asignados.

Existe un conjunto importante de protocolos que opera a partir del Nivel de Red y hasta el nivel de Aplicación del Modelo OSI (al que nos referiremos posteriormente) proporcionando un servicio básico de transmisión de datos que puede ser orientado a la conexión o no orientado a la conexión.

Los protocolos orientados a conexión constan de tres fases diferentes:

- Establecimiento de la conexión: durante esta fase se envía un paquete con características diferentes a los paquetes de datos, que se encarga de establecer la ruta que seguirán los paquetes de datos. Este paquete lleva la dirección origen y destino de los datos.

- Transferencia de datos: en esta fase se intercambian los paquetes de datos, los cuales no llevan ni dirección origen ni dirección destino de los datos ya que viajan por una trayectoria preestablecida.

- Liberación de la conexión; durante esta fase se envía un paquete con características diferentes a los paquetes de datos, que se encarga de liberar la conexión cuando la transmisión de datos haya concluido. Este paquete lleva la dirección origen y destino de los datos.

Cada una de estas fases involucra a los dos host que se quieren comunicar y el servicio de transferencia de datos por sí mismo.

Un protocolo orientado a la conexión es un servicio de transferencia de datos secuencial y seguro. Aunque la conexión permanezca establecida durante mucho tiempo, el transmisor asume que cada mensaje es recibido exitosamente y en el mismo orden en que fueron enviados. Si los mensajes se pierden, se duplican, o no llegan en orden, la conexión es liberada y esto se le informa a todos los dispositivos relacionados con la conexión. La liberación de la conexión puede

ocurrir en cualquier momento por una de las partes comunicantes o por el mismo protocolo. Esto es una propiedad inherente de los protocolos orientados a conexión, pues cada una de las tres fases de las que consta el protocolo puede fallar independientemente en cualquier momento.

Los protocolos no orientados a conexión están formados por una sola fase. Ellos aceptan los paquetes que van a ser transmitidos y tratan de entregarlos de la mejor forma posible. El proceso de usuario dirige el paquete hacia el software del protocolo e identifica al proceso destino, hacia el cual el paquete es enviado. El software del protocolo es el encargado de entregar el paquete a su destino. Cada mensaje debe especificar su receptor y es manipulado independientemente de los otros paquetes.

Con un protocolo no orientado a la conexión no se obtiene un servicio de transferencia de datos seguro y ordenado, pues no existen procedimientos que detecten los errores, ni se envían las señales de reconocimiento que indican la validación del mensaje. Esto provoca que los mensajes no lleguen en orden, puesto que no todos viajan por las mismas rutas a través de la inter-red, que se pierdan si hay congestión en la vía o hubo errores en la transmisión o que se dupliquen al no recibirse la confirmación de la llegada del mensaje, y por lo tanto los procesos del nivel de transporte lo reenvían. Esto es proporcionado por protocolos de un nivel superior o por los programas que se estén comunicando. En una arquitectura de niveles, el usuario de un protocolo que ejecuta en un nivel en particular, es un proceso que trabaja en el nivel superior.

2.2.7 Modelo OSI

Debido a la gran diversidad de arquitecturas de redes y de protocolos de comunicación la Organización Internacional de Estandarización (ISO) se dio a la tarea de desarrollar un proyecto ambicioso que describiera las bases de la interconexión de sistemas, la forma en que las máquinas pueden intercambiar información y una definición flexible de los niveles funcionales que forman a la computadora. Así nació, a principio de los años 80, el modelo OSI (Modelo de Interconexión de Sistemas Abiertos).

El modelo de referencia OSI rápidamente cambió el modelo de arquitectura primario para la comunicación entre computadoras. Aunque otros modelos de arquitectura han sido creados, la mayoría de los vendedores de red relacionan sus productos con el modelo OSI, cuando ellos quieren educar a los usuarios acerca de estos. Es por eso que para un buen aprendizaje de la tecnología de la red, el modelo OSI es la mejor herramienta.

El modelo OSI está estructurado por 7 capas diferentes, físico, enlace, red, transporte, sesión, presentación, aplicación, cada una con una tarea específica que es ofrecida a las capas adyacentes. El modo de implementar la tarea es propio de cada capa. Los niveles más bajos están implementados en software y hardware; los cinco restantes están implementados en software.

La siguiente figura muestra lo dicho anteriormente.

Nivel de Aplicación
Nivel de Presentación
Nivel de Sesión
Nivel de Transporte
Nivel de Red
Nivel de Enlace
Nivel Físico

Tabla 2 Modelo OSI

2.2.7.1 Arquitectura del Modelo OSI

A continuación mostraremos los niveles que forman el modelo OSI con sus características:

Nivel de Aplicación Es el tope del modelo OSI donde residen los procesos que pueden ser accesados por el usuario. En esta capa cada usuario determina qué programa desarrollar y qué protocolo utilizar para la comunicación con las computadoras remotas. Realiza las funciones de transferencia de ficheros, terminal virtual, ejecución remota, correo electrónico, acceso a bases de datos remotas, etc. La unidad de datos que intercambia es el mensaje.

Nivel de Presentación Está relacionado con la preservación del contenido de la información de los datos transmitidos en la red.

	Debe negociar una sintaxis común para la transferencia de los mensajes. Realiza las funciones de compresión de textos, encriptamiento, conversión de alfabetos, conversión entre ficheros de distinto formato.
Nivel de Sesión	Con este nivel el usuario interactúa para gestionar el establecimiento de la conexión y debe manejar de forma eficiente el diálogo entre las máquinas o estaciones homólogas. Su unidad de intercambio es el mensaje.
Nivel de Transporte	La función de esta capa es garantizar un servicio de transporte de datos confiable entre las dos estaciones que se comunican. Este nivel debe realizar el reordenamiento de los paquetes, evitar la duplicación así como el almacenamiento excesivo de los paquetes de los paquetes para conformar los mensajes, que son su unidad de intercambio.
Nivel de Red	Se encarga del enrutamiento de los paquetes, subdivide los mensajes en paquetes y le agrega la información necesaria para que ocurra el enrutamiento de los paquetes a través de la subred de comunicación.

Nivel de Enlace Es el responsable de la transmisión de los datos sobre el enlace de un sistema a otro y controla el mecanismo de la transmisión de las tramas. Su función principal es, chequear, detectar y corregir los errores de bits.

Nivel Físico Define las características de hardware necesarias para transportar las señales de datos que se emiten tales como niveles de voltaje, número y localización de los pines de la interfaz, etc. La unidad de intercambio es el bit.

2.2.8 Conmutadores (Switch)

Los conmutadores controlan el flujo del tráfico de red basándose en la información de la dirección de cada paquete. Un conmutador averigua qué dispositivos están conectados a sus puertos (monitorizando los paquetes que recibe), y envía los paquetes al puerto adecuado solamente. Esta acción permite la comunicación simultánea a través del conmutador, con lo que se mejora el ancho de banda poseen una memoria interna en donde se guarda las direcciones MAC de todos los equipos que a él están conectados. A esta base de datos se le conoce como Switch DataBase

2.2.7.1 Características de los Switches

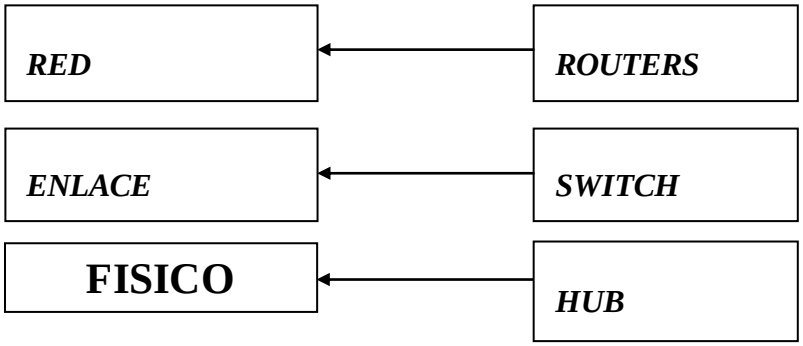


Tabla 3 Características de Switches

- Operan a Nivel de la Capa de Enlace por lo que la comunicación en estos es independiente del protocolo.
- Permite a través de una matriz de conmutadores el establecimiento de trayectorias simultáneas que posibilitan varias comunicaciones a la vez.
- Además de regenerar la señal ejecutan la selección de ruta a nivel de enlace, lo que aumenta considerablemente el rendimiento de la red.
- Conectan las estaciones formando una sola red muy grande pero con tráfico segmentado, lo que permite aislar los dominios de colisiones.
- Atendiendo a la dirección destino, transmiten sólo en esa dirección.
- Ven la red como una única red lógica por lo que necesitan un salto para llegar al destino.

2.2.7.2 Como Trabajan los Switches?

Los switches de las Redes Ethernet utilizan un sistema denominado “puentes transparente” para crear sus tablas de direcciones o bases de datos, esta es una tecnología que le permite al switch conocer todo lo concerniente a la localización de los nodos a él conectados en la Red sin necesidad de que el administrador de la misma tenga nada que hacer al respecto.

Esta Tecnología se compone de 5 partes:

- aprendizaje.
- inundación.
- Filtrado.
- Reenvío.
- Envejecimiento.

2.2.8 HISTORIA DE LA COMUNICACIÓN INALÁMBRICAS

Aunque la tecnología se conoce como redes de área local inalámbricas en realidad se trata de tecnología de radio. Por tanto, no obstante que la historia de Wi-Fi u 802.11 solo existe a partir de mediados de la década de los ochenta, en realidad esta tecnología comenzó aproximadamente 100 años atrás. Del mismo modo en que la tecnología de radiodifusión es el fundamento de la LAN inalámbrica los primeros trabajos en electromagnética, a su vez representan los fundamentos de la radio.

Las primeras LAN inalámbricas en 1985, gracias a los cambios en las regulaciones de la Parte 15 de la FCC que permitieron el uso de radio a través del espectro extendido en las aplicaciones comerciales, se abrió la puerta para comercializar la tecnología. Poco después de un año de que se efectuaran los cambios en la regulación FCC, se creó en Toronto una compañía, Telesystems SLW, para explotar este desarrollo.

Es interesante observar que aunque el sistema diseñado por Telesystems en realidad era un espectro extendido, usaba una variación de este tema, que es distinta del sistema de cambio de frecuencia que inicialmente incluía la patente original del espectro extendido. En lugar de hacer que la señal de banda angosta saltara de una frecuencia a la siguiente a través de un ancho de banda establecido, Telesystems empleó un sistema que se conoce como secuencia directa, donde una señal de banda angosta se extiende a través del ancho de banda determinado al multiplicador el ancho de la señal a través de un conjunto de frecuencia más grande.

El resultado de este sistema es similar al del salto de frecuencias; es decir, la señal de banda angosta que se extiende a través de un ancho de banda más amplio es menos susceptible a las interferencias, debido a que sólo una parte de la señal multiplicada necesita alcanzar al receptor esperando para que la transmisión sea exitosa. Además, y de manera muy parecida al salto de frecuencia, la señal de secuencia directa proporcionaba en ese momento el mismo nivel de seguridad, en la medida que la capacidad disminuida por unidad del ancho de banda hacía que la

señal fuera menos discernible del ruido circundante cuando se usaba equipo de interferencia moderno.

En 1988 fue introducido al mercado el primer sistema comercial basado en la tecnología secuencia directa en el espectro extendido (Direct Sequence Spread Spectrum – DSSS), Además de incorporar DSSS, estos sistemas no operaban en una banda licenciada, sino que trabajaban sobre una banda sin licencia establecida recientemente por la FCC alrededor de 902 y 928 Mhz. Debido a que esta banda estaba ubicada cerca de la banda licenciada para los teléfonos celulares analógicos que se usan en Norteamérica, proporcionó a los fabricantes la ventaja de construir sus dispositivos libres de licencia con componentes existentes para nuevos propósitos y que originalmente estaban destinados para el uso de teléfonos celulares.

Los primeros productos de Telesystems fueron diseñados como reemplazos del cableado, ya sea para conectar múltiples computadoras de escritorio con una estación de base central de manera muy parecida en la que funcionaría una red Ethernet, o para conectar las redes en edificios separados de modo semejante que funciona un puente, no obstante que la operación de la banda de 900 Mhz se proporcionó para una infraestructura común a través de Estados Unidos, Canadá y Australia, estaba limitada en el sentido que no estaba asignada para la operación sin licencia en otras partes del mundo.

Para llegar a los mercados ubicados fuera de cada áreas, los fabricantes comenzaron a producir radios que operaban en la parte de 2.4 Ghz del espectro de frecuencia que estaba disponible para la operación libre de licencia a lo largo de la mayor parte de Europa y Japón además de Estados Unidos, Canadá y Australia. De modo similar al de la banda de 900 Mhz, la de 2.4 Ghz proporciono a los fabricantes la ventaje de usar componentes existentes que originalmente estaban destinados para el uso de teléfonos celulares europeos que operaban en una banda con licencia aproximada.

2.2.9 COMO TRABAJAN LAS REDES INALAMBRICAS

Utilizan ondas electromagnéticas para transportar información de un punto a otro sin necesidad de una conexión física. Las ondas de radio frecuencia a menudo se refieren como portadoras de radio, debido a que su única función consiste en entregar la energía que conllevan al receptor remoto.

Los datos que se desean transmitir se superponen sobre la portadora de forma tal que en el lado receptor puedan ser precisamente recuperados, este proceso es conocido como "modulación de la portadora", por la información que se desea transmitir. Una vez que la portadora ha sido modulada, la señal de radio ocupa más de una frecuencia, ya que la frecuencia de la información moduladora se añade a la portadora.

Pueden existir varias portadoras en el mismo espacio de forma simultánea, sin interferirse mutuamente, siempre y cuando se transmitan en diferente frecuencia. Para extraer los datos, el receptor de radio se sintoniza para seleccionar una frecuencia de radio y rechazar señales en otras frecuencias.

En la configuración típica de una WLAN, un dispositivo transmisor/receptor (denominado punto de acceso) se conecta a la red alambrada desde un punto fijo utilizando un cable Ethernet estándar.

Como mínimo, el punto de acceso recibe, almacena y transmite los datos entre la red inalámbrica y la red alambrada. Uno de estos dispositivos puede soportar un grupo pequeño de usuarios (hasta 30 por punto de acceso) dentro de un rango promedio de 30 a 100 metros.

La distancia sobre la cual los dispositivos de radio frecuencia se pueden comunicar depende del diseño de los productos, las interacciones con los objetos típicos de construcción, y aún las personas pueden afectar la forma de propagación de las ondas.

El punto de acceso o la antena asociada al punto de acceso usualmente se monta en un punto alto, sin embargo, puede colocarse en cualquier lugar práctico, siempre y cuando se obtenga la cobertura deseada.

Los usuarios finales acceden la WLAN a través de adaptadores inalámbricos, implementados en tarjetas PC para computadoras portátiles (Laptops), adaptadores ISA o PCI para computadoras de escritorio (Desktops) o mediante adaptadores totalmente integrados en asistentes personales digitales (PDA, por las siglas de Personal Digital Assistant). Los adaptadores WLAN proporcionan la interfaz entre el sistema operativo de red del cliente y las ondas electromagnéticas por conducto de la antena. La naturaleza de la conexión inalámbrica es transparente al sistema operativo de red.

2.2.9.1. WI-FI (SIN CABLES)

Wi-Fi es un nombre comercial desarrollado por un grupo de comercio industrial llamado Wi-Fi Alliance ellos describen los productos de redes de área local inalámbrico basados en los estándares 802.11 IEEE y está diseñado para que tenga un nombre más accesible para los usuarios de la misma manera que Ethernet y Token Ring son más fáciles de aprender que 802.3 y 802.5 IEEE respectivamente.

En principio Wi-Fi fue creado para describir sólo los dispositivos con velocidades máximas de 11 Mbps que operaban en la porción de 2.4 Ghz del espectro de frecuencia y que cumplían con las especificaciones 802.11b IEEE. Más tarde se decidió que Wi-Fi debería ser extendido para incluir los productos con velocidades de datos máximas de 54 Mbps que operan en la porción de 2.4 Ghz y

5 Ghz del espectro de frecuencia y que están basados en las especificaciones 802.11 y 802.11a del IEEE

2.2.9.2 ORGANISMO DE ESTANDARIZACIÓN INTERNACIONAL

Las redes inalámbricas o WN básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE (Organismo de estandarización internacional).

802.11a: Fue la primera aproximación a las WN y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por Punto de Acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (posibilidades de aseguro de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos

multimedia online), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la HyperLAN2 y la parcial disponibilidad de la misma en Japón.

802.11b: Es la segunda aproximación de las WN. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2.4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA.

Adolece de varios de los inconvenientes que tiene el 802.11a como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2.4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth, lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE

802.11g: Es la tercera aproximación a las WN, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps. Se

encuentra en estado de borrador en el IEEE, se prevee que se estandarice para mediados de 2003. Funciona dentro de la frecuencia de 2.4 Ghz.

Dispone de los mismos inconvenientes que el 802.11b además de los que pueden aparecer por la aún no estandarización del mismo por parte del IEEE (puede haber incompatibilidades con dispositivos de diferentes fabricantes).

Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

2.2.10. DISPOSITIVOS WIRELESS

Dispositivos Tarjetas de red, o TR, que serán los que tengamos integrados en nuestro ordenador, o bien conectados mediante un conector PCMCIA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa. SUBSTITUYEN a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Dispositivos Puntos de Acceso, ó PA, los cuales serán los encargados de recibir la información de los diferentes TR de los que conste la red bien para su centralización bien para su encaminamiento. COMPLEMENTAN a los Hubs,

Switches o Routers, si bien los PAs pueden sustituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

2.2.11. TOPOLOGÍAS

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

En el mundo Wireless existen dos topologías básicas:

Topología Ad-Hoc. Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí.

Topología Infraestructura, en el cual existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todos los demás (Tarjetas de Red Wifi). Este nodo

sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP.

Un caso especial de topología de redes inalámbricas es el caso de las redes Mesh, que se verá más adelante.

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

Modo Managed, es el modo en el que el TR se conecta al AP para que éste último le sirva de concentrador. El TR sólo se comunica con el AP.

Modo Master. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP/OPENAP.

Esta afirmación se ve confirmada al descubrir que muchos APs en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como TR.

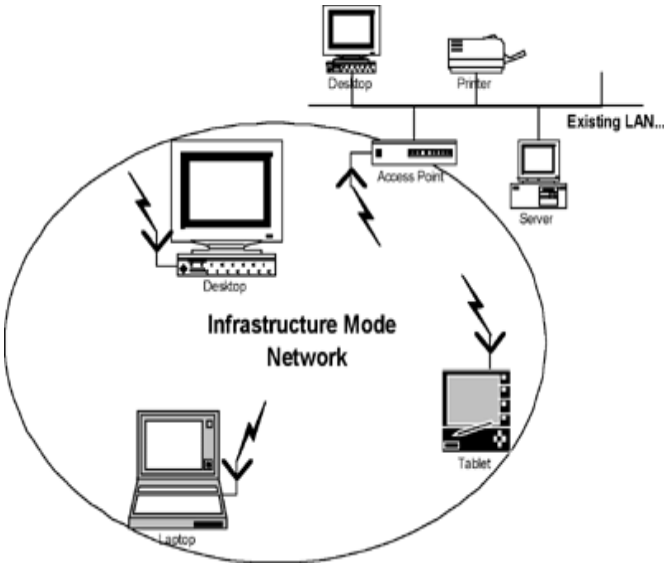


Grafico: 6 Topología Infraestructura

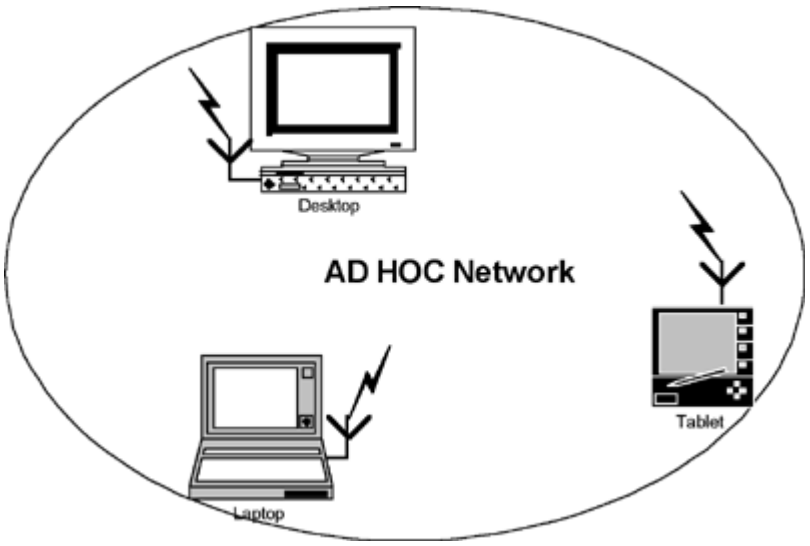


Grafico: 2 Topología Ad-Hoc

2.2.12. SEGURIDAD EN LAS COMUNICACIONES WIRELESS

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

2.2.13 Terminología

Para poder entender la forma de implementar mejor la seguridad en una red wireless, es necesario comprender primero ciertos elementos:

WEP. Significa Wired Equivalet Privacy, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

OSA vs SKA. OSA (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. SKA (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la

misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

ACL. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

CNAC. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

SSID. Significa Service Set IDentifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

Pasos para asegurar una red inalámbrica

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático.

Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi

nadie puede significar que es segura en un 99.99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red wireless. Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar desperdigando la información hacia los cuatro vientos con todo lo que esto conlleva.

Paso 1.- Debemos activar el WEP. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

Paso 2.- Debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono

Paso 3.- Uso del OSA. Esto es debido a que en la autenticación mediante el SKA, se puede comprometer la clave WEP, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

Paso 4.- Desactivar el DHCP y activar el ACL. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

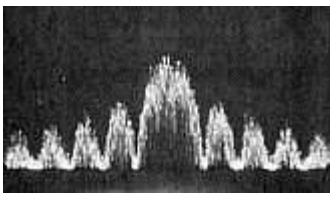
Paso 5.- Cambiar el SSID y modificar su intervalo de difusión. Cada casa comercial configura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

Paso 6.- Hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

Paso 7.- Aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente el IEEE está trabajando en la definición del estándar 802.11i que permita disponer de sistemas de comunicación entre dispositivos wireless realmente seguros. También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

2.2.14. Espectro disperso (Spread Spectrum)



A Spectrum Analyzer Photo of a Direct Sequence (DS) Spread Spectrum signal

A Spectrum Analyzer Photo of a Frequency Hop (FH) Spread Spectrum signal

Grafico: 3 Espectro disperso

.

Spread Spectrum es una técnica de comunicación que por los altos costes que acarrea, se aplicó casi exclusivamente para objetivos militares, hasta comienzos de los años noventa. Sin embargo, comienza a surgir lentamente un mercado comercial. Seguramente mucha gente ha escuchado alguna vez nombrar a LAN (Local Area Networks: Area de redes locales).

Estas son redes que comunican ordenadores entre sí a través de cables, lo que hace posible que por ordenador se pueda enviar correo dentro de un edificio determinado, por ejemplo. Actualmente se venden también 'Radio LAN' (RLAN), que constituyen una comunicación inalámbrica entre una cantidad determinada de ordenadores.

Para poder captar un programa radial hay que sintonizar con un emisor que está en una determinada frecuencia. Emisores diferentes están en diferentes frecuencias. Cada emisor ocupa un pequeño trozo de la banda emisora dentro de la cual se concentra la potencia de emisión irradiada. Ese trocito, también llamado amplitud de banda, tiene que ser lo suficientemente grande como para que los emisores

cercanos no sean interferidos. A medida que la amplitud de banda es más angosta, pueden funcionar más emisores en una banda de frecuencia.

Un ejemplo:

La banda emisora FM cubre la zona de frecuencia de 88-108 Mhz. Si la amplitud de banda de un emisor es 1 Mhz, entonces pueden caber (108-88)/1 = 20 emisores en la banda emisora FM.

Si la amplitud de banda de un emisor es 0,2 Mhz (= 200 Khz), entonces pueden caber (108-88)/0,2 = 100 emisores en la banda emisora FM.

Si ahora, por ejemplo, quisiéramos colocar 200 emisores en la banda emisora FM, eso sólo se podría si la amplitud de banda de cada emisor disminuyera. Sin embargo, esto ocasiona problemas porque en la emisora FM se maneja una amplitud de banda de 200 Khz. Una amplitud de banda más pequeña produce una menor transmisión de información por lo cual es imposible obtener una calidad Hifi. Este principio no es sólo válido para la banda emisora FM,sino también para otras bandas de frecuencia como la banda emisora AM, bandas de radioaficionados, bandas de la policía, etc.

La radio-receptora se puede sintonizar siempre en una frecuencia. Esa frecuencia es retransmitida por el emisor con una amplitud de banda lo más pequeña posible,

pero lo suficientemente grande como para transmitir la información deseada. Este tipo de receptores se llama receptores de banda angosta (estrecha).

Por el contrario, en Spread Spectrum no se elige por una amplitud de banda lo más pequeña posible, sino justamente por una lo más grande posible. La amplitud de banda es mayor de lo que se necesita estrictamente para la transmisión de la información. Esta mayor amplitud de banda puede obtenerse de dos maneras. La primera es codificar la información con una señal seudo-fortuita (aleatoria)(1).

La información codificada se transmite en la frecuencia en que funciona el emisor para lo cual se utiliza una amplitud de banda mucho mayor que la que se usa sin codificación (secuencia directa). La segunda posibilidad es codificar la frecuencia de trabajo con una señal seudo-fortuita(aleatoria), por lo que la frecuencia de trabajo cambia permanentemente. En cada frecuencia se envía un trocito de información (Frecuencia Hopping).
Esta difusión a través del Spread Spectrum puede ser tan grande que un receptor-radio sólo capta un zumbido. Un receptor-radio 'oye', pues, sólo una pequeña parte de la banda de frecuencia. Para poder captar la señal dispersa se necesita receptores con amplitud de banda especial que transformen el zumbido recibido en información. Este receptor de banda ancha tiene que disponer del decodificador apropiado para transformar la señal del emisor en información.

De lo anterior se puede deducir en forma sencilla porqué los militares están tan interesados en esta técnica. A eso se agrega que es difícil interferir un emisor de

este tipo. Si se interfiere toda la banda de frecuencia, se vuelve imposible cualquier radiocomunicación Determinados emisores de escuchas hacen uso también del principio Spread Spectrum. Las ondas de radio están sumergidas en el zumbido (ruido de fondo), en el Spread Spectrum, por lo cual el emisor no es fácil de descubrir con la ayuda de los aparatos de detección corrientes.

La expectativa general es que comercialmente se vaya a ir haciendo cada vez más uso de Spread Spectrum para la transmisión de datos. A causa de que la potencia de emisión se difunde sobre una banda ancha, puede ser usada por encima de bandas de frecuencia existentes, sin interferir la recepción de banda angosta. Por eso es posible admitir más usuarios en una banda de frecuencia. Otra ventaja es la seguridad de la comunicación. Al fin y al cabo, la información se envía cifrada.

En un sistema RLAN con 100 usuarios que utilizan Spread Spectrum es suficiente con 1 frecuencia emisora y 100 señales-codificadoras diferentes. La información se codifica, entonces, directamente.
La técnica Spread Spectrum se puede usar sobre bandas de frecuencia diferentes. Walkie-talkies en el trabajo o teléfonos inalámbricos en casa son aplicaciones que desde el punto de vista técnico se esperan en el porvenir. Sin embargo, este tipo de aparatos no están aún comercializados o son apenas adquiribles (o están a la venta en forma reducida).

La aplicación de esta técnica podría caer fuera del sistema de permisos de emisión, debido a que para un receptor de banda angosta parece como si hubiera

zumbido y las emisoras radiales normales en su conjunto, no sufren interferencias por la técnica Spread Spectrum. En los Estados Unidos se admitió sin permiso oficial un sistema RLAN del fabricante NCR (2). Se espera que a fines de 1994 el Instituto europeo para telecomunicaciones estándar (ETSI) fijará el estándar en relación con RLAN para una banda de frecuencia (2,4 - 2,4835 Ghz) después de lo cual probablemente el gobierno holandés legislará sobre eso. A largo plazo el consumidor tendría que poder tener acceso sin más rodeos a los aparatos Spread Spectrum aprobados por las autoridades.

Cómo influirá la revisión de la ley de Telecomunicaciones y la amenazante prohibición de los aparatos criptográficos y/o el entregar claves codificadas sobre el uso de los aparatos Spread Spectrum no está todavía totalmente claro. La HDTP (Dirección General de Telecomunicaciones y Correos) declaró a petición que no esperaba que los propósitos políticos fueran a influir sobre las RLAN, que se usan dentro de casa.

La reglamentación de la criptografía tendría que ver sobre todo, según la HDTP, con el uso de la red digital de teléfonos de coches. Dentro del recientemente conocido proyecto de ley en relación con la criptografía no fueron nombradas categorías de excepción, sin embargo. Sobre este proyecto ha caído, sin embargo, tanta crítica que seguramente no será aprobado en su forma actual.

2.2.13 ANTENAS.- Definición

Grafico: 4 Antenas

La antena es un elemento fundamental de cualquier instalación de radio, siendo tan importante, que de ella depende que la señal llegue hasta donde tenemos previsto con el mayor nivel y calidad que sea posible.

Es un conjunto de conductores debidamente asociados, que se emplea tanto para la recepción como para la transmisión de ondas electromagnéticas, que comprenden los rayos gamma, los rayos X, la luz visible y las ondas de radio.

2.2.14 Características De Las Antenas

Resistencia de radiación: Debido a la radiación en las antenas se presenta pérdida de potencia. Por ello se ha establecido un parámetro denominado resistencia de radiación Rr , cuyo valor podemos definir como el valor de una

resistencia típica en la cual, al circular la misma corriente que circula en la antena, disipara la misma cantidad de potencia.

Eficiencia de una antena: Se conoce con el nombre de eficiencia de una antena (rendimiento) a la relación existente entre la potencia radiada y la potencia entregada a la misma.

Impedancia de entrada de una antena: En general, la impedancia de entrada de la antena dependerá de la frecuencia, estando formada por una componente activa Re, y una reactiva Xe. De esta forma, Re se puede asimilar a la resistencia total de la antena en sus terminales de entrada. Generalizando, podemos decir entonces que la impedancia de entrada de la antena es simplemente la relación entre el voltaje de entrada de la antena y la corriente de entrada.

Ganancia de una antena: La ganancia de una antena representa la capacidad que tiene este dispositivo como radiador. Es el parámetro que mejor caracteriza la antena. La forma más simple de esquematizar la ganancia de una antena es comparando la densidad de potencia radiada en la dirección de máxima radiación con el valor medio radiado en todas las direcciones del espacio, ofreciéndose en términos absolutos.

Aquellas antenas que radian por igual en todas las direcciones se llaman isotrópicas y su ganancia es de 1. Basados en esta definición, podemos hablar de la ganancia como la relación entre la potencia y campo eléctrico producido por la

antena (experimental) y la que producirá una antena isotrópica (referencia), la cual radiará con la misma potencia.

Longitud eficaz de la antena: Sobre una antena se inducen corrientes y voltajes. Por tal razón, a la antena receptora se le puede considerar como un generador ideal de voltaje (V), con una impedancia interna que resulta ser igual a la de entrada.

Polarización de la antena: La onda electromagnética posee el campo eléctrico vibrando en un plano transversal a la dirección de propagación, pudiendo tener diversas orientaciones sobre el mismo. La polarización de la antena hace referencia a la orientación del campo eléctrico radiado. De esta forma, si un observador en un punto lejano a la antena "visualizara" el campo eléctrico lo podría mirar de las siguientes formas:

Describiendo una elipse. En este caso se dice que la onda esta polarizada elípticamente.

Describiendo una circunferencia (polarización circular). Polarización horizontal o vertical, describiendo una línea recta. Es importante anotar que, para que una antena "responda" a una onda incidente, tiene que tener la misma polarización que la onda. Por ejemplo, un dipolo vertical responderá a una onda incidente si la polarización de dicha onda es vertical también.

Ancho de haz de una antena: Podemos hablar del ancho de haz de una antena como el espaciamiento angular entre dos puntos determinados de potencia media (-3dB), ubicándolos con respecto a la posición del lóbulo principal perteneciente al patrón de radiación de la antena.

Ancho de banda de la antena: Se puede describir como los valores de frecuencia para los cuales la antena desarrolla su trabajo de manera correcta. De igual forma, el ancho de banda de una antena depende de las condiciones de los puntos de potencia media.

La naturaleza de las ondas cuando los electrones oscilan en un circuito eléctrico, parte de su energía se convierte en radiación electromagnética. La frecuencia (la rapidez de la oscilación) debe ser muy alta para producir ondas de intensidad aprovechable que, una vez formadas, viajan por el espacio a la velocidad de la luz. Cuando una de esas ondas encuentra una antena metálica, parte de su energía pasa a los electrones libres del metal y los pone en movimiento, formando una corriente alterna cuya frecuencia es la misma que la de la onda.

Este es, sencillamente, el principio de la comunicación por radio, existen diferentes modos de propagación que pueden surgir como el resultado del lanzamiento de ondas electromagnéticas al espacio por medio de antenas de configuración adecuada. Si no existiera el aire ni las capas ionosféricas, esto es, en el vacío, las ondas de radio viajarían en línea recta. Sin embargo, debido a la presencia de gases de diferente composición en la atmósfera terrestre, la propagación de ondas se ve influenciada por una serie diversa de mecanismo.

El modo de propagación más sencillo es aquel en que la onda sigue una trayectoria recta entre la antena de transmisión y la de recepción. A este tipo de onda se le conoce como directa o de línea de visión, LOS (Line Of Sight). Las microondas son el ejemplo clásico de este mecanismo de propagación. En condiciones óptimas las microondas pueden considerarse como un haz concentrado de energía electromagnética que hace la travesía desde la antena de emisión hasta la recepción desplazándose en línea recta. Más aún, debido a las longitudes de onda tan pequeñas en esta modalidad de aplicación, las antenas utilizadas, reflectores parabólicos, y en general todo el esquema de propagación, pueden analizarse como si fuera un sistema de características ópticas

2.2.15. ANTENAS PARA REDES INALAMBRICAS WIFI

Disponemos de tres tipos de antenas para redes inalámbricas:

Antenas direccionales (o directivas)

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz de luz concreto y estrecho 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 "escucha" nada, no se puede establecer comunicación entre los interlocutores.

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

Grafico: 5 Antenas Direccionales

Antenas unidireccionales

Orientan la señal en todas direcciones con un haz 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 de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Grafico: 6 Antenas Unidireccional

Antenas sectoriales

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

sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

Grafico: 7 Antenas Sectorial

Apertura vertical y apertura horizontal

La apertura es cuanto se "abre" el haz de la antena. El haz emitido o recibido por una 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 los 40º y una antena sectorial oscilará entre los 90º y los 180º.

La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbrica mente. 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.

¿Qué antenas debemos instalar?

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores. Las antenas sectoriales se suelen utilizan cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa.

Si necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque por ejemplo) lo más probable es que utilice una antena omnidireccional. Si tiene que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo un PC que está bastante lejos) utilizará una antena direccional, finalmente, si necesita dar cobertura amplia y a la vez a larga distancia, utilizará antenas sectoriales.

2.2.16. MEDIOS DE TRANSMISIÓN

Punto de acceso (Access Point):

Se suele abreviar como AP. Piensa en ellos como un HUB de red normal: a él se conectan los equipos y es él quien reparte los paquetes. Pues en WIFI es algo similar, es un dispositivo que 'gestiona', los paquetes lanzados por otras estaciones inalámbricas, haciéndolas llegar a su destino. Además el punto de acceso, da conectividad a una red cableada, por lo que la red inalámbrica puede acceder a otros equipos que estuvieran en una red cableada.

Grafico: 8 Access Point

Bridges o Puentes

Al igual que un repetidor, un bridge puede unir segmentos o grupos de trabajo LAN. Sin embargo, un bridge puede, además, dividir una red para aislar el tráfico o los problemas. Por ejemplo, si el volumen del tráfico de uno o dos equipos o de un departamento está sobrecargando la red con los datos y ralentizan todas las operaciones, el bridge podría aislar a estos equipos o al departamento.

- Los bridges se pueden utilizar para:
- Extender la longitud de un segmento.
- Proporcionar un incremento en el número de equipos de la red.

- Reducir los cuellos de botella del tráfico resultantes de un número excesivo de equipos conectados.
- Dividir una red sobrecargada en dos redes separadas, reduciendo la cantidad de tráfico en cada segmento y haciendo que la red sea más eficiente.
- Enlazar medios físicos diferentes como par trenzado y Ethernet coaxial.

Los bridges trabajan a nivel de enlace de datos del modelo de referencia OSI y, por tanto, toda la información de los niveles superiores no está disponible para ellos. Más que distinguir entre un protocolo y otro, los bridges pasan todos los protocolos que aparecen en la red. Todos los protocolos se pasan a través de los bridges, de forma que aparecen en los equipos personales para determinar los protocolos que pueden reconocer.

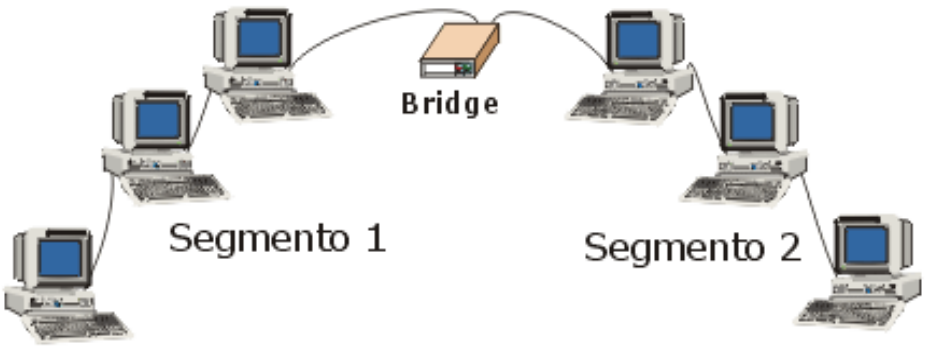


Grafico: 9 Bridges

Los bridges trabajan en el nivel MAC y, por ello, algunas veces se conocen como bridges de nivel MAC.

Un bridge de nivel MAC:

- Escucha todo el tráfico.
- Comprueba las direcciones origen y destino de cada paquete.
- Construye una tabla de encaminamiento, donde la información está disponible.
- Reenvían paquetes de la siguiente forma:
- Si el destino no aparece en la tabla de encaminamiento, el bridge reenvía el paquete a todos los segmentos.
- Si el destino aparece en la tabla de encaminamiento, el bridge reenvía el paquete al segmento correspondiente (a menos que este segmento sea también el origen).

Un bridge funciona considerando que cada nodo de la red tiene su propia dirección. Un bridge reenvía paquetes en función de la dirección del nodo destino.

Realmente, los bridges tienen algún grado de inteligencia puesto que aprenden a dónde enviar los datos. Cuando el tráfico pasa a través del bridge, la información sobre las direcciones de los equipos se almacena en la RAM del bridge. El bridge utiliza esta RAM para generar una tabla de encaminamiento en función de las direcciones de origen.

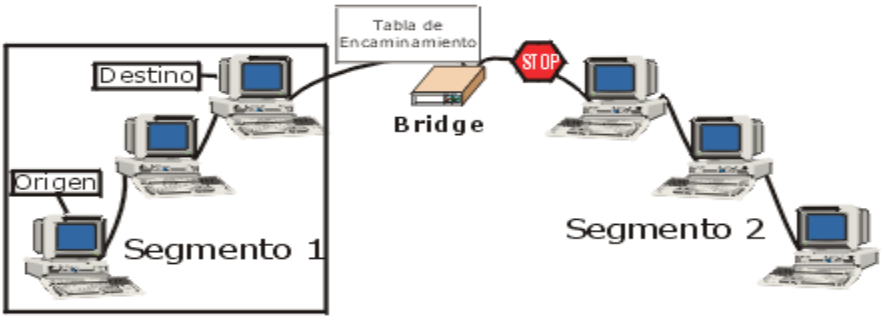


Grafico: 10 Bridges

Inicialmente, la tabla de encaminamiento del bridge está vacía. Cuando los nodos transmiten los paquetes, la dirección de origen se copia en la tabla de encaminamiento. Con esta información de la dirección, el bridge identifica qué equipos están en cada segmento de la red.

Creación de la tabla de encaminamiento. Los bridges generan sus tablas de encaminamiento en función de las direcciones de los equipos que han transmitido datos en la red. Los bridges utilizan, de forma específica, las direcciones de origen (dirección del dispositivo que inicia la transmisión) para crear una tabla de encaminamiento.

Cuando el bridge recibe un paquete, la dirección de origen se compara con la tabla de encaminamiento. Si no aparece la dirección de origen, se añade a la tabla. A continuación, el bridge compara la dirección de destino con la base de datos de la tabla de encaminamiento.

- Si la dirección de destino está en la tabla de encaminamiento y aparece en el mismo segmento de la dirección de origen, se descarta el paquete. Este filtrado ayuda a reducir el tráfico de la red y aislar segmentos de la red.
- Si la dirección de destino está en la tabla de encaminamiento y no aparece en el mismo segmento de la dirección de origen, el bridge envía el paquete al puerto apropiado que permite alcanzar la dirección de destino.
- Si la dirección de destino no está en la tabla de encaminamiento, el bridge envía el paquete a todos sus puertos, excepto al puerto desde donde se originó el envío.

Resumiendo, si un bridge conoce la localización del nodo de destino, envía el paquete a dicha localización. Si no conoce el destino, envía el paquete a todos los segmentos.

Segmentación del tráfico de red. Un bridge puede segmentar el tráfico mediante su tabla de encaminamiento. Un equipo en el segmento 1 (origen), envía datos a otro equipo (destino) también localizado en el segmento 1. Si la dirección de destino está en la tabla de encaminamiento, el bridge puede determinar que el equipo destino está también en el segmento 1. Dado que los equipos origen y destino están en el mismo segmento 1, se tiene que el paquete no se reenvía a través del bridge al segmento 2.

Por tanto, los bridges pueden utilizar las tablas de encaminamiento para reducir el tráfico de la red controlando los paquetes que se envían al resto de los segmentos.

Este control (o restricción) del flujo del tráfico de red se conoce como «segmentación del tráfico de red».

Una red grande no está limitada a un solo bridge. Se pueden utilizar múltiples bridge para combinar diferentes redes pequeñas en una red más grande.

Los bridges tienen todas las características de los repetidores, pero también proporcionan más ventajas. Ofrecen mejor rendimiento de red que los repetidores. Las redes unidas por bridges se han dividido y, por tanto, un número menor de equipos compiten en cada segmento por los recursos disponibles.

Visto de otra forma, si una gran red Ethernet se dividió en dos segmentos conectados por un bridge, cada red nueva transportaría un número menor de paquetes, tendríamos menos colisiones y operaría de forma mucho más eficiente. Aunque cada red estaría separada, el bridge pasaría el tráfico apropiado entre ellas.

Routers

Grafico: 11 Router

En un entorno que está formado por diferentes segmentos de red con distintos protocolos y arquitecturas, el bridge podría resultar inadecuado para asegurar una comunicación rápida entre todos los segmentos. Una red de esta complejidad necesita un dispositivo que no sólo conozca las direcciones de cada segmento, sino también, que sea capaz de determinar el camino más rápido para el envío de datos y filtrado del tráfico de difusión en el segmento local. Este dispositivo se conoce como router

Un **router,** enrutador o encaminador es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

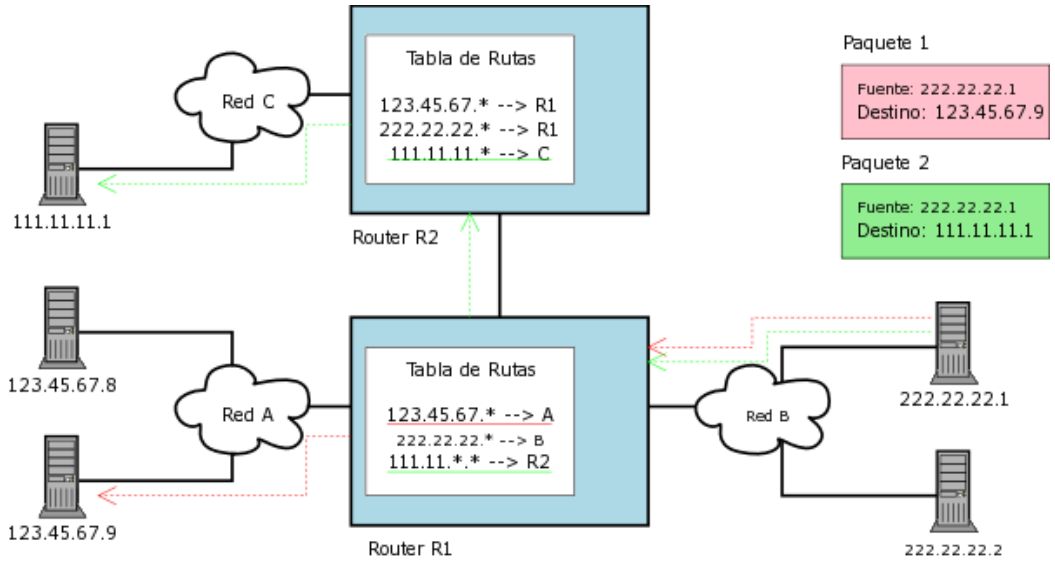


Grafico: 12 Capa de red

Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Los routers leen en el paquete la información de direccionamiento de las redes complejas teniendo acceso a información adicional, puesto que trabajan a un nivel superior del modelo OSI en comparación con los bridges.

Los routers pueden proporcionar las siguientes funciones de un bridge:

- Filtrado y aislamiento del tráfico.
- Conexión de segmentos de red.

Los routers tienen acceso a más información en los paquetes de la que tienen los bridges y utilizan esta información para mejorar la entrega de los paquetes. Los routers se utilizan en redes complejas puesto que proporcionan una mejor gestión

del tráfico. Los routers pueden compartir con otro router el estado y la información de encaminamiento y utilizar esta información para evitar conexiones lentas o incorrectas.

Los routers mantienen sus propias tablas de encaminamiento, normalmente constituidas por direcciones de red; también se pueden incluir las direcciones de los hosts si la arquitectura de red lo requiere. Para determinar la dirección de destino de los datos de llegada, las tablas de encaminamiento incluyen:

Todas las direcciones de red conocidas.

- Instrucciones para la conexión con otras redes.
- Los posibles caminos entre los routers.
- El coste de enviar los datos a través de estos caminos.

Un router utiliza sus tablas de encaminamiento de datos para seleccionar la mejor ruta en función de los caminos disponibles y del coste. La tabla de encaminamiento que mantiene un bridge contienen las direcciones del subnivel MAC para cada nodo, mientras que la tabla de encaminamiento que mantiene un router contiene números de red. Aunque los fabricantes de ambos tipos de equipamiento han seleccionado utilizar el término «tabla de encaminamiento», tienen diferente significado para cada uno de los dispositivos.

Los routers requieren direcciones específicas. Entienden sólo los números de red que les permiten comunicarse con otros routers y direcciones NIC locales. Los routers no conversan con equipos remotos.

Cuando los routers reciben paquetes destinados a una red remota, los envían al router que gestiona la red de destino. En algunas ocasiones esto constituye una ventaja porque significa que los routers pueden:

- Segmentar grandes redes en otras más pequeñas.
- Actuar como barrera de seguridad entre los diferentes segmentos.
- Prohibir las «tormentas» de difusión, puestos que no se envían estos mensajes de difusión.

Los routers son más lentos que los bridges, puesto que deben realizar funciones complejas sobre cada paquete. Cuando se pasan los paquetes de router a router, se separan las direcciones de origen y de destino del nivel de enlace de datos y, a continuación, se vuelven a generar. Esto activa a un router para encaminar desde una red Ethernet TCP/IP a un servidor en una red Token Ring TCP/IP.

Dado que los routers sólo leen paquetes direccionados de red, no permiten pasar datos corruptos a la red. Por tanto, al no permitir pasar datos corruptos ni tormentas de difusión de datos, los routers implican muy poca tensión en las redes.

Los routers no ven la dirección del nodo de destino, sólo tienen control de las direcciones de red. Los routers pasarán información sólo si conocen la dirección de la red. Esta capacidad de controlar el paso de datos a través del router reduce la cantidad de tráfico entre las redes y permite a los routers utilizar estos enlaces de forma más eficiente que los bridges.

La utilización de un esquema de direccionamiento basado en router permite a los administradores poder dividir una gran red en muchas redes separadas, y dado que los routers no pasan e incluso controlan cada paquete, actúan como una barrera de seguridad entre los segmentos de la red. Esto permite reducir bastante la cantidad de tráfico en la red y el tiempo de espera por parte de los usuarios.

Protocolos que permiten encaminar. No todos los protocolos permiten encaminar.

Los protocolos que encaminan son:

- DECnet.
- Protocolo de Internet (IP).
- Intercambio de paquetes entre redes (IPX).
- OSI.
- Sistema de red de Xerox (XNS).
- DDP (Apple Talk).

Los protocolos que no pueden encaminar son:

- Protocolo de transporte de área local (LAT), un protocolo de Digital Equipment Corporation.
- NetBEUI (Interfaz de usuario extendida NetBIOS).

Los routers pueden utilizar en la misma red múltiples protocolos.

Selección de los caminos. A diferencia de los bridges, los routers pueden establecer múltiples caminos activos entre los segmentos LAN y seleccionar entre los caminos redundantes. Los routers pueden enlazar segmentos que utilizan paquetes de datos y acceso al medio completamente diferentes, permitiendo utilizar a los routers distintos caminos disponibles. Esto significa que si un router no funciona, los datos todavía se pueden pasar a través de routers alternativos.

Un router puede escuchar una red e identificar las partes que están ocupadas. Esta información la utiliza para determinar el camino sobre el que envía los datos. Si un camino está ocupado, el router identifica un camino alternativo para poder enviar los datos.

Un router decide el camino que seguirá el paquete de datos determinando el número de saltos que se generan entre los segmentos de red. Al igual que los bridges, los routers generan tablas de encaminamiento y las utilizan en los siguientes algoritmos de encaminamiento:

- OSPF (Primer camino abierto más corto) es un algoritmo de encaminamiento basado en el estado del enlace. Los algoritmos de estado de enlace controlan el proceso de encaminamiento y permiten a los routers responder rápidamente a modificaciones que se produzcan en la red.

- RIP (Protocolo de información de encaminamiento) utiliza algoritmos con vectores de distancia para determinar la ruta. El Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) e IPX admite RIP.

- NLSP (Protocolo de servicios de enlace NetWare) es un algoritmo de estado de enlace a utilizar con IPX.

Tipos de routers

Los tipos principales de routers son:

- Estático. Los routers estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.
- Dinámico. Los routers dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración. Son más sofisticados que los routers estáticos, examinan la

información de otros routers y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

Características de los dos tipos de routers

Routers estáticos	**Routers dinámicos**
Instalación y configuración manual de todos los routers	Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.
Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento	Pueden seleccionar una ruta en función de factores tales como coste y cantidad del tráfico de enlace.
Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.	Pueden decidir enviar paquetes sobre rutas alternativas.
Se consideran más seguros puesto que los administradores especifican cada ruta	Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones.

Gateways

Los gateways activan la comunicación entre diferentes arquitecturas y entornos. Se encargan de empaquetar y convertir los datos de un entorno a otro, de forma que cada entorno pueda entender los datos del otro entorno. Un gateway empaqueta información para que coincida con los requerimientos del sistema destino. Los gateways pueden modificar el formato de un mensaje para que se ajuste al programa de aplicación en el destino de la transferencia. Por ejemplo, los gateways de correo electrónico, como el X.400, reciben mensajes en un formato, los formatean y envían en formato X.400 utilizado por el receptor, y viceversa.

Un gateway enlaza dos sistemas que no utilizan los mismos:

- Protocolos de comunicaciones.
- Estructuras de formateo de datos.
- Lenguajes.
- Arquitectura.

Los gateways interconectan redes heterogéneas; por ejemplo, pueden conectar un servidor Windows NT de Microsoft a una Arquitectura de red de los sistemas IBM (SNA). Los gateways modifican el formato de los datos y los adaptan al programa de aplicación del destino que recibe estos datos.

Los gateways son de tarea específica. Esto significa que están dedicados a un tipo de transferencia. A menudo, se referencia por su nombre de tarea (gateway Windows NT Server a SNA).

Un gateway utiliza los datos de un entorno, desmantela su pila de protocolo anterior y empaqueta los datos en la pila del protocolo de la red destino.

Para procesar los datos, el gateway:

- Desactiva los datos de llegada a través de la pila del protocolo de la red.
- Encapsula los datos de salida en la pila del protocolo de otra red para permitir su transmisión.

Algunos gateways utilizan los siete niveles del modelo OSI, pero, normalmente, realizan la conversión de protocolo en el nivel de aplicación. No obstante, el nivel de funcionalidad varía ampliamente entre los distintos tipos de gateways.

Una utilización habitual de los gateways es actuar como traductores entre equipos personales y mini equipos o entornos de grandes sistemas. Un gateway en un host que conecta los equipos de una LAN con los sistemas de mini equipo o grandes entornos (mainframe) que no reconocen los equipos conectados a la LAN.

En un entorno LAN normalmente se diseña un equipo para realizar el papel de gateway. Los programas de aplicaciones especiales en los equipos personales acceden a los grandes sistemas comunicando con el entorno de dicho sistema a través del equipo gateway. Los usuarios pueden acceder a los recursos de los grandes sistemas sólo cuando estos recursos están en sus propios equipos personales.

Normalmente, los gateways se dedican en la red a servidores. Pueden utilizar un porcentaje significativo del ancho de banda disponible para un servidor, puesto que realizan tareas que implican una utilización importante de recursos, tales como las conversiones de protocolos. Si un servidor gateway se utiliza para múltiples tareas, será necesario adecuar las necesidades de ancho de banda y de RAM o se producirá una caída del rendimiento de las funciones del servidor.

Los gateways se consideran como opciones para la implementación, puesto que no implican una carga importante en los circuitos de comunicación de la red y realizan, de forma eficiente, tareas muy específicas.

2.2.17 GESTION COMERCIAL

Para **PALAFOX Gustavo (2005)** la gestión comercial de las pequeñas y medianas empresa está basada en la calidad de sus servicios y sus ventas, mejorarlas será de gran interés para todos los pequeños y micro empresarios que desean sobresalir ante la competencia que en la actualidad es muy agresiva. A

veces las empresas dan mayor interés a la administración de cómo dirigir, administrar los recursos económicos, humanos y materiales; dejando al otro lado el servicio al cliente y que cada día toma más importancia para crecer en un mercado competitivo.

Por descuidar esta área tan importante que está en el departamento de ventas podemos perder muchos clientes debido por el mal trato a nuestra cliente, mientras que nuestra competencia sigue conquistando mercados y nuevas clientelas debido al buen servicio y atención que le brinda; para determinar que servicios son los que el cliente demanda se deben realizar encuestas periódicas que permitan identificar los posibles servicios a ofrecer y ver que estrategias y técnicas utilizaremos. El servicio al cliente es una potente herramienta de marketing que nos facilita conocer a nuestra clientela y sus necesidades y para ello contamos con los siguientes elementos:

- Contacto cara a cara
- Relación con el cliente
- Correspondencia
- Reclamos y cumplimientos
- Instalaciones

La importancia del servicio[1] al cliente es poder llegar a nuestra clientela con una poderosa venta promocional, los descuentos, la oferta y el apoyo al cliente en el desarrollo de nuevas estrategias para reducir los costos de inventario y

[1] CALDERON Neyra, "Servicio al cliente", www.gestiopolis.com

prever contingencias para no perjudicar más adelante nuestra empresa y de nuestro cliente.

Las acciones y actitudes se reflejan en el comportamiento de las distintas personas con las cuales el cliente entra en contacto produciendo un impacto sobre el nivel de satisfacción del cliente incluyendo, la cortesía general con el que el personal maneja las preguntas, los problemas, como ofrece o amplía la información, provee servicio y la forma como trata a los otros clientes.

El cliente interno es un cliente cautivo que trae problemas y dificultades en el trabajo, mientras que el cliente externo trae satisfacciones y beneficios para la empresa de las cuales se beneficiaran los dueños y los que laboran en ella, por tales razones los que trabajan en la empresa deben de atender o tratar de la mejor manera al cliente es decir como a un rey. El problema es que cada área de la empresa ve al cliente desde su perspectiva, sin una visión integral y a veces haciendo comentarios como a continuación mencionamos.

- **Vendedor.-** Cliente es un ladrón que tiene dinero y debe devolvérmelo.
- **Almacén.-** Cliente es aquel que viene a desorganizar mis inventarios.
- **Departamento Legal.-** Cliente es aquel que puede demandarnos si nos descuidamos.
- **Producción.-** Cliente ¿qué es eso?
- **Atención a los clientes.-** Cliente es esa persona que sólo viene a quejarse.

- **Gerente.-** Cliente es esa persona que constantemente me interrumpe y me quita tiempo de las cosas importantes.
- **Propietario.-** Cliente es una persona caprichosa que tengo que aguantarle para que me ingrese dinero.

2.2.15.1 Comercialización

El concepto de comercialización significa que una organización encamina todos sus esfuerzos a satisfacer a sus clientes por una ganancia. La comercialización se ocupa de aquello que los clientes desean, y debería servir de guía para lo que se produce y se ofrece.

Hay tres ideas fundamentales incluidas en la definición del concepto de comercialización:

1. Orientación hacia el cliente.
2. Esfuerzo total de la empresa.
3. Ganancia como objetivo.

Para obtener una comercialización efectiva significa entregar los bienes y servicios que los consumidores desean y necesitan. Significa conseguirles los productos en el momento oportuno, en el lugar adecuado y a precio conveniente.

Las funciones universales de la comercialización son: comprar, vender, transportar, almacenar, estandarizar y clasificar, financiar, correr riesgos y lograr información del mercado. El intercambio suele implicar compra y

venta. La función de compra significa buscar y evaluar bienes y servicios. La función venta requiere promover el producto. La función de transporte se refiere a trasladar. La función de almacenamiento implicar guardar los productos de acuerdo con el tamaño y calidad. Estandarizar y clasificar incluyen ordenar los productos de acuerdo con el tamaño y calidad. La financiación provee el efectivo y crédito necesarios para operar.(producir, vender, comprar, almacenar. La toma de riesgos entraña soportar las incertidumbres que forman parte de la comercialización.

2.2.15.2 Que es Venta

Se define a la venta como el proceso personal o impersonal de ayudar y /o persuadir a un cliente potencial para que adquiera un producto o servicio o actúe a un favor de una idea comercialmente significativa para el vendedor.

Ventas Personales

La venta personal es definida como la comunicación personal de información para convencer a alguien de que compre algo.

Ventajas

- Generalmente se centra en los compradores potenciales, con lo cual se reduce al mínimo la pérdida de tiempo.
- Busca realizar una venta; otras formas de promoción tiene el objeto de estimular al prospecto para que compre.

Desventajas

- Personal Inadecuado; Algunas empresas no siempre cuentan con el personal adecuado que permita logar ventas exitosas.

Tipos de Personal

Existen dos tipos de venta personal

- Venta de Mostrador: Es aquella en la que los consumidores acuden al vendedor.
- Fuerza Externa de Ventas: Es aquella en la que el vendedor acude al cliente.

2.2.15.3 Que es un producto

Cada empresa está vendiendo algo que el cliente desea: satisfacción, uso o beneficio. Cuando los productores o intermediarios compran productos, se interesan en la ganancia que puede obtener de su compra, mediante su uso o reventa, no en cómo se hicieron los productos.

Debido a que los consumidores compran satisfacción, no elementos sueltos. Producto significa el ofrecimiento por una firma de satisfacer necesidades. Lo que interesa a los clientes es como ellos ven el producto.

La calidad del producto también debería determinarse a través de como los clientes ven el producto. Desde una perspectiva comercial, calidad significa la capacidad de un producto para satisfacer las necesidades o requerimientos de un cliente.

2.3.- Idea a defender y Variables

"Con la implementación de una red Hibrida se mejorará la gestión de ventas en la empresa Mora & hijos"

Variables:

Variable Independiente: Red Hibrida

Variable Dependiente: Gestión de ventas

CAPITULO III

MARCO METODOLÓGICO

3.1 MODALIDAD DE LA INVESTIGACIÓN

El objetivo de cualquier ciencia es adquirir conocimientos y la elección del método adecuado que nos permita conocer la realidad es por tanto fundamental. El problema surge al aceptar como ciertos los conocimientos erróneos o viceversa. Los métodos inductivos y deductivos tienen objetivos diferentes y podrían ser resumidos como desarrollo de la teoría y análisis de la teoría respectivamente. Los **métodos inductivos** están generalmente asociados con la investigación cualitativa mientras que el **método deductivo** está asociado frecuentemente con la investigación cuantitativa.

La **investigación cuantitativa** es aquella en la que se recogen y analizan datos cuantitativos sobre variables. La **investigación cualitativa** evita la cuantificación. Los investigadores cualitativos hacen registros narrativos de los fenómenos que son estudiados mediante técnicas como la observación participante y las entrevistas no estructuradas. La diferencia fundamental entre ambas metodologías es que la cuantitativa estudia la asociación o relación entre variables cuantificadas y la cualitativa lo hace en contextos estructurales y situacionales. La investigación cualitativa trata de identificar la naturaleza profunda de las realidades, su sistema de relaciones, su estructura dinámica.

La investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede. Tras el estudio de la asociación o correlación pretende, a su vez, hacer inferencia causal que explique por qué las cosas suceden o no de una forma determinada.

3.2 TIPOS DE INVESTIGACIÓN.

Se utilizaran algunos tipos de investigación como:

3.2.1 Investigación bibliográfica

Se caracteriza por usas, en forma predominante, la información obtenida de libros, revistas, periódicos y documentos en general.

La información se obtiene mediante la lectura científica de los textos se recoge utilizando la técnica del fichaje bibliográfico y mnemotécnico y acudiendo a las bibliotecas, donde se encuentran concentradas las fuentes de información bibliográfica

La investigación bibliográfica constituye un punto de partida para la realización del proceso de investigación, ya que permite analizar y evaluar aquello que se ha investigado y lo que falta por indagar del objeto o fenómeno de estudio.

3.3.2 Investigación de campo

Emplea básicamente la información obtenida a través de las técnicas de la observación, entrevista y cuestionario.

Las técnicas de investigación de campo utilizan sus propios procedimientos e instrumentos para la recolección de datos, junto a los mecanismos específicos de control y valides de la información.

La utilización predominante de las técnicas de investigación de campo no excluye la posibilidad y necesidad de emplear determinada información bibliográfica de apoyo a la investigación.

3.3 POBLACIÓN Y MUESTRA

La población está constituida por todos los involucrados en el problema y así tenemos:

FUNCIÓN	N.- DE PERSONAS
Administradores	2
Empleados	10
Clientes	65
TOTAL	75

La muestra está constituida por un porcentaje de la población, en este caso como la población es reducida procedemos a tomar toda ella como la muestra a investigar en este problema.

3.4 MÉTODOS, TÉCNICAS E INSTRUMENTOS

Se aplicara el método inductivo deductivo para resolver un problema en particular y extenderlo a lo general.

En cuanto a las técnicas para recopilar información tenemos: **la encuesta, la entrevista y la observación**

Los instrumentos que apoyaran dichas técnicas son: **el cuestionario, la guía de entrevista y la libreta de notas.**

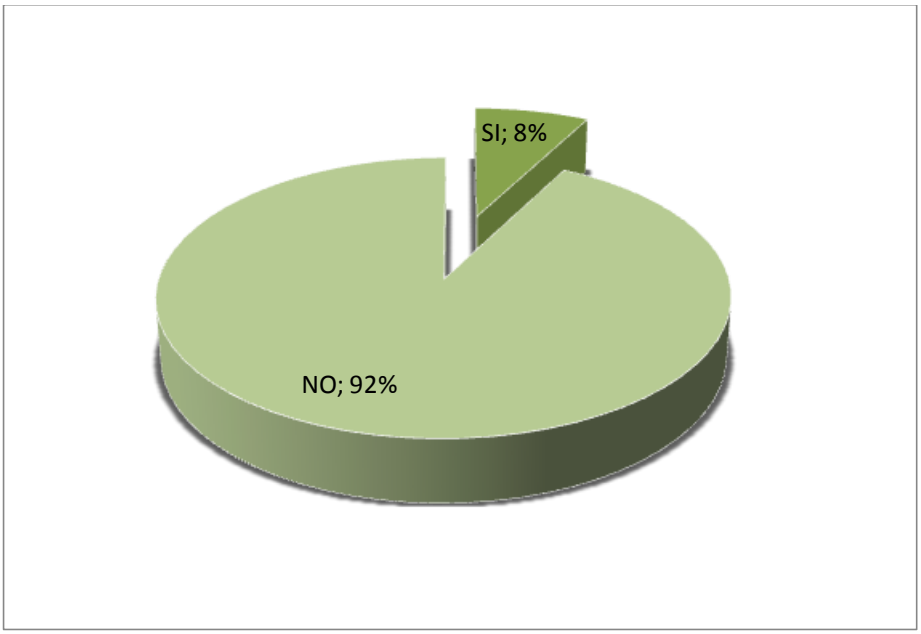
3.5 INTERPRETACIÓN DE DATOS

Tabulamos los datos de la encuesta realizada a los clientes.

1. La oficina central tiene actualizado el inventario de la agencia?

SI		**NO**	
%	**Valor**	**%**	**Valor**
8	5	92	60

Tabla 3 Datos de la pregunta 1

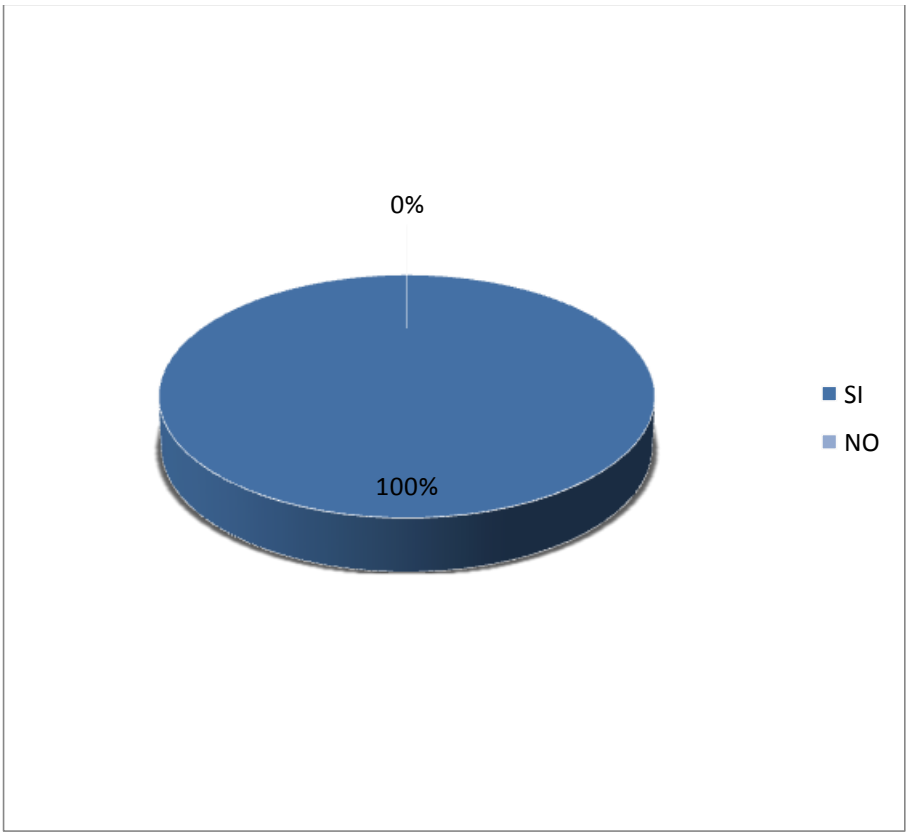


El noventa y dos por ciento de los clientes indican que la oficina central no mantiene un inventario actualizado de la agencia.

2. Se carece de un medio de comunicación inmediato entre la agencia principal y la sucursal?

SI		**NO**	
%	**Valor**	**%**	**Valor**
100	65	0	0

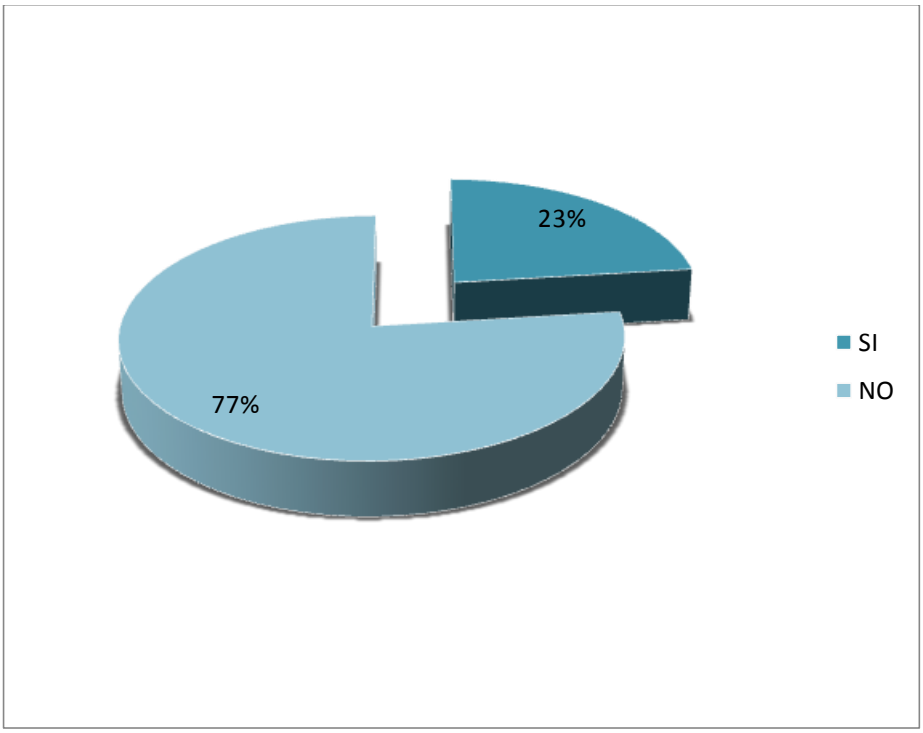
Tabla 4 Datos de la pregunta 2



El cien por ciento de los clientes indican que no existe un medio de comunicación de datos entre la sucursal y la agencia principal.

3. Cree usted que la información que genera las diferentes áreas de la empresa y agencias es confiable para las estadísticas?

SI		**NO**	
%	**Valor**	**%**	**Valor**
23	15	77	50

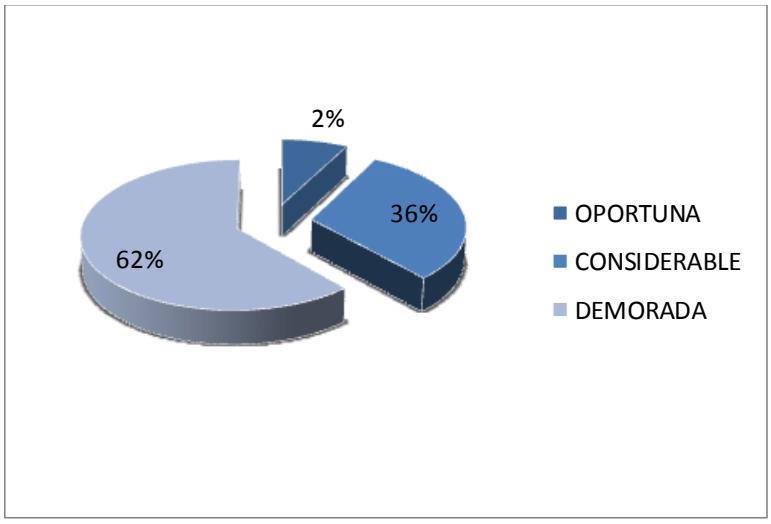


El setenta y siete por ciento de los clientes internos indican que no es confiable la información para los cálculos estadísticos por la demora en consolidar la información

4. Considera usted que el tiempo de la información requerida llega de manera oportuna, considerable, demorada?

OPORTUNA		**CONSIDERABLE**		**DEMORADA**	
%	**Valor**	**%**	**Valor**	**%**	**Valor**
7	5	31	20	62	40

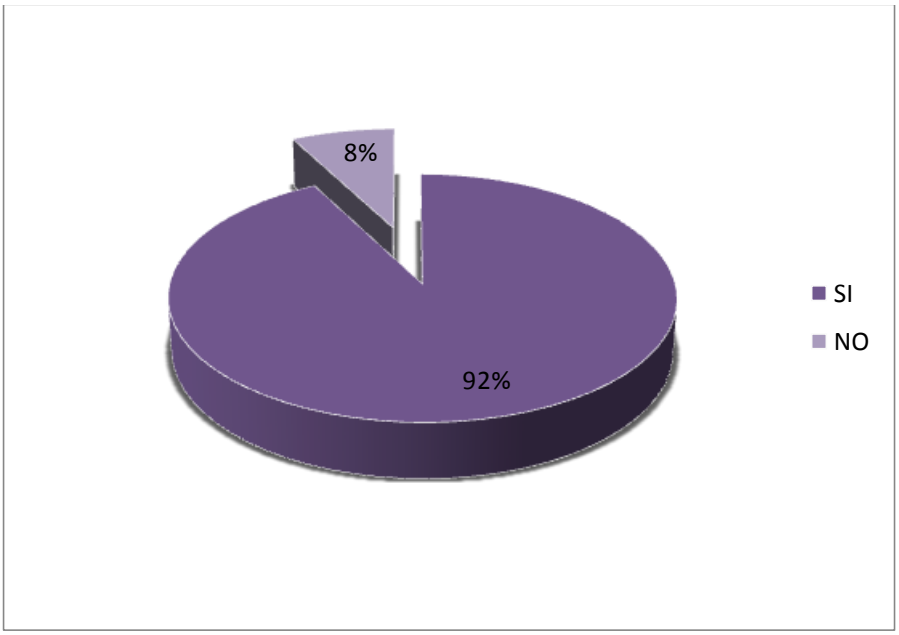
Tabla 6 Datos de la pregunta 4



Como podemos apreciar existe un 62 por ciento de los clientes indican que la información es demorada para realizar sus tareas y análisis.

5. Cree usted que al no existir una red de datos entre la matriz y la sucursal influya en la gestión comercial de la empresa?

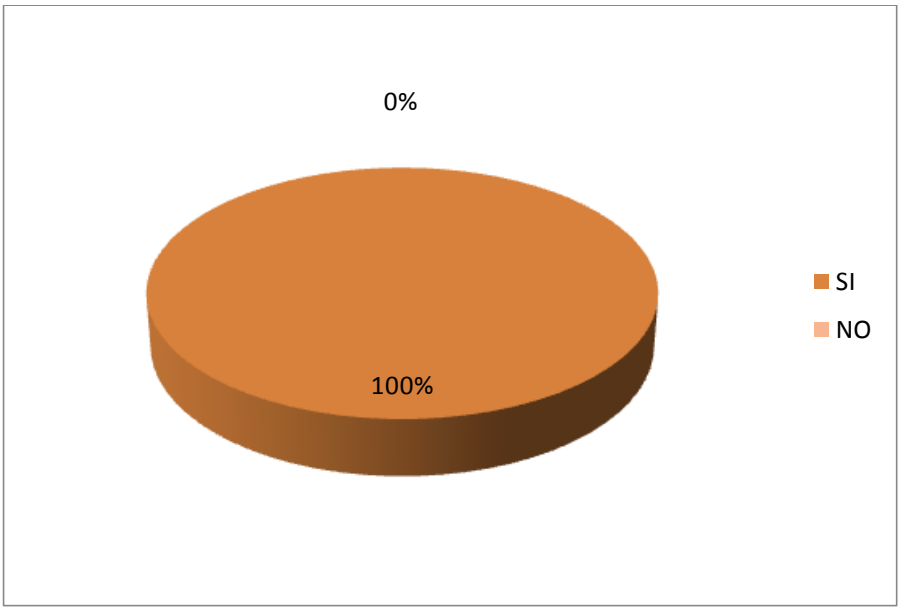
SI		**NO**	
%	**Valor**	**%**	**Valor**
92	60	8	5



El noventa y dos por ciento de los clientes indican que si influye en la gestión comercial el no tener una red de datos entre la matriz y la sucursal.

6. Considera usted necesario la instalación de un sistema de comunicaciones inalámbricas que permita la consolidación de la información de todos sus centros?

SI		NO	
%	Valor	%	Valor
100	65	0	0

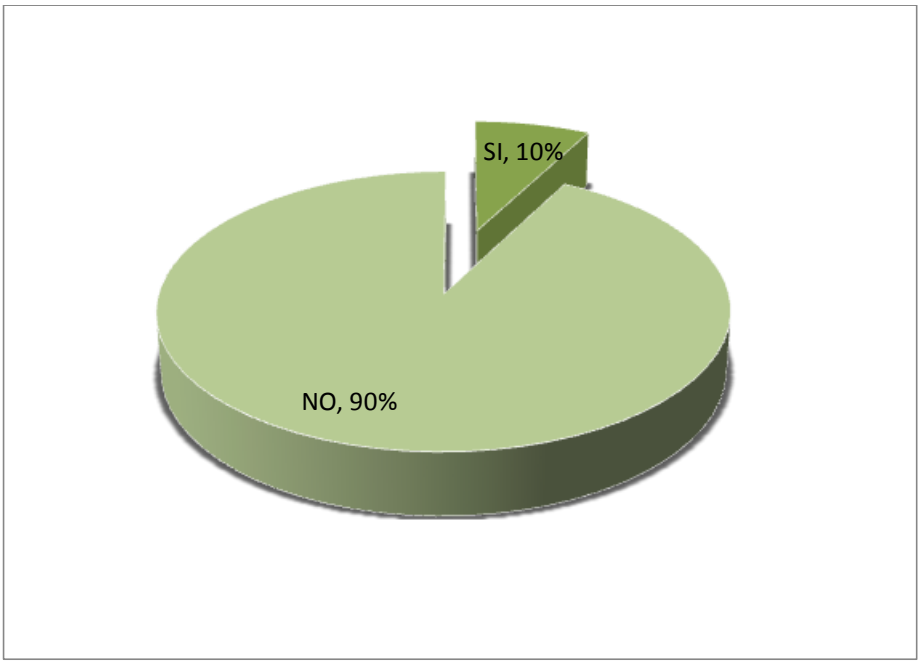


Es necesario aplicar un sistema de comunicaciones que nos permita integrar todos los centros y agencias para consolidación de la información, existe un cien por ciento que está de acuerdo.

Tabulamos los datos de la encuesta realizada a los empleados

1. La oficina central tiene actualizado el inventario de las agencias?

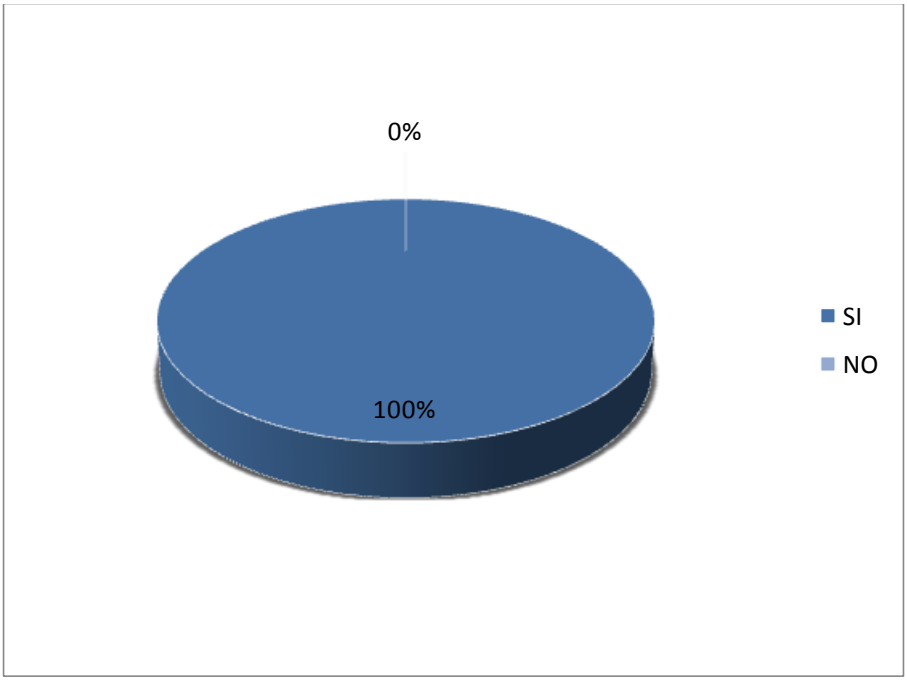
SI		**NO**	
%	**Valor**	**%**	**Valor**
10	1	90	9



El noventa por ciento de los empleados indican que la oficina central no mantiene un inventario actualizado de las agencias.

2. Se carece de un medio de comunicación inmediata entre la agencia principal y las sucursales?

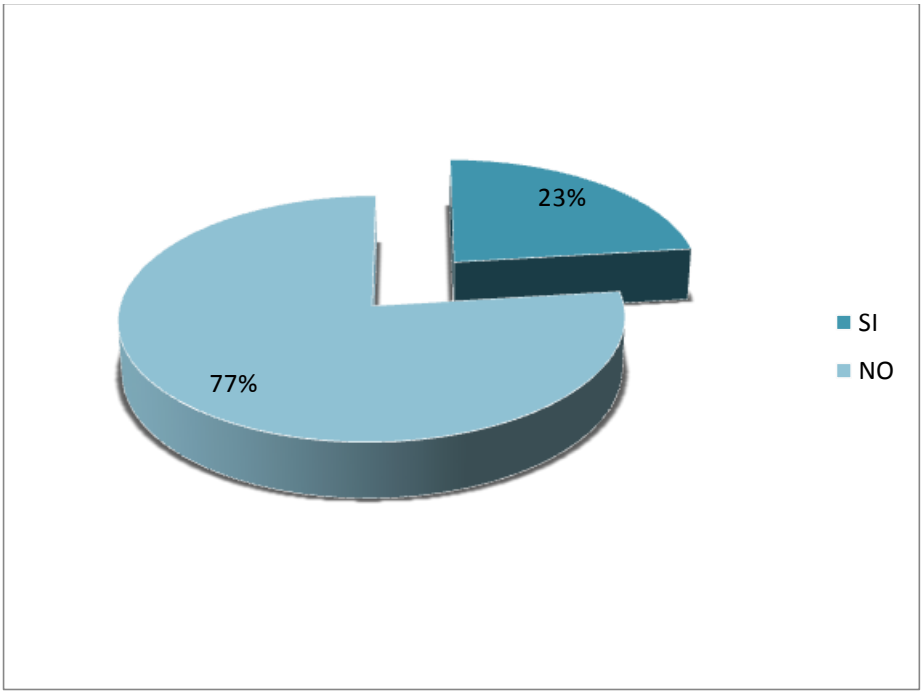
SI		NO	
%	Valor	%	Valor
100	10	0	0



El cien por ciento de los empleados indican que no existe un medio de comunicación de datos entre las sucursales y la agencia principal.

3. Cree usted que la información que genera las diferentes áreas de la empresa y agencias es confiable para las estadísticas?

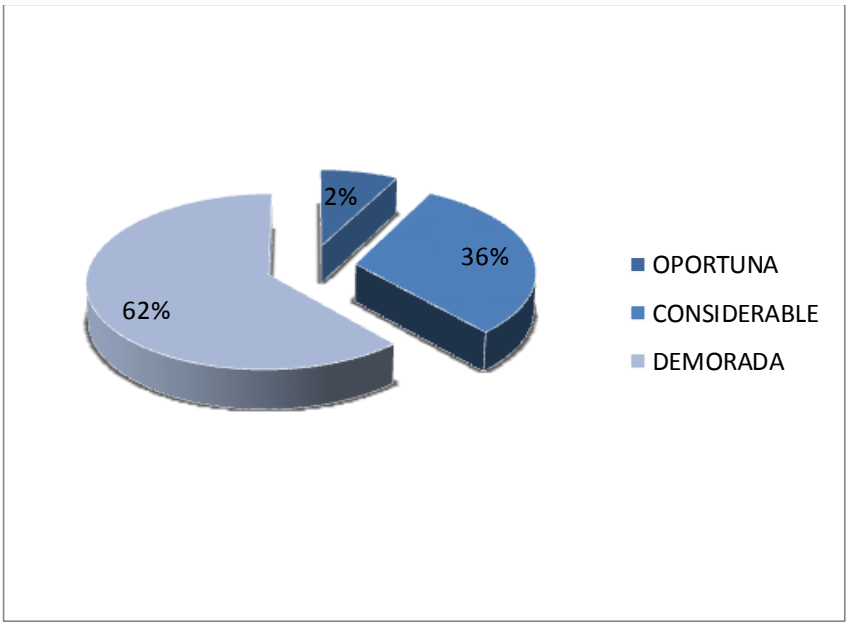
SI		NO	
%	Valor	%	Valor
23	2	77	8



El 77% por ciento de los empleados internos indican que no es confiable la información para los cálculos estadísticos

4. Considera usted que el tiempo de la información requerida llega de manera oportuna, considerable, demorada?

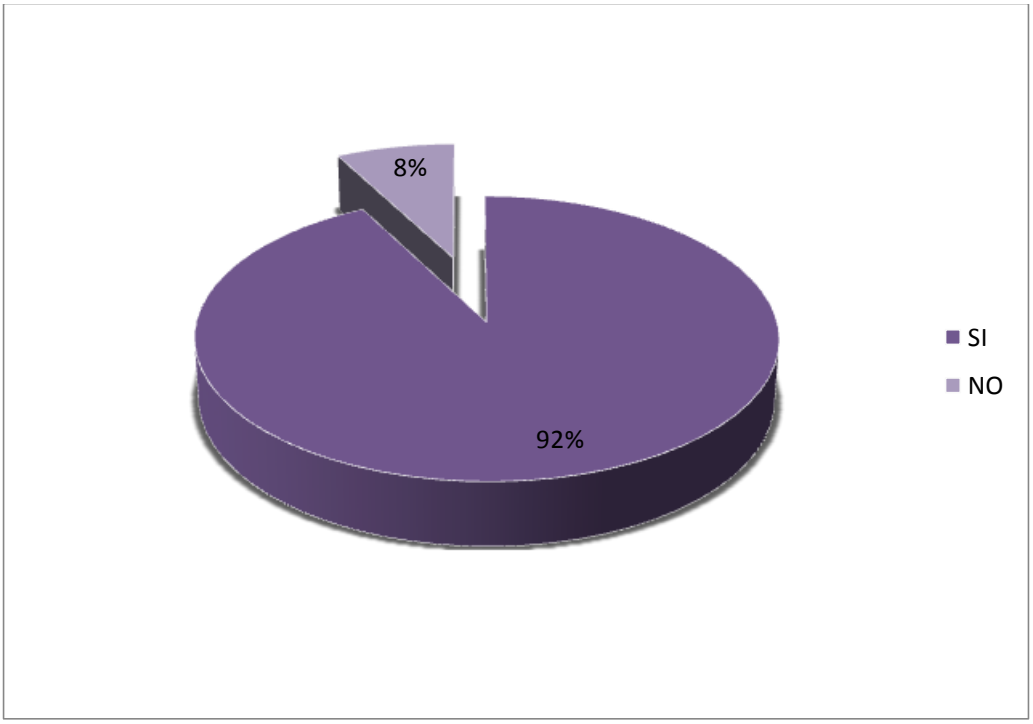
OPORTUNA		CONSIDERABLE		DEMORADA	
%	**Valor**	**%**	**Valor**	**%**	**Valor**
2	5	36	3	62	2



Como podemos apreciar existe un 62 por ciento de los clientes internos indican que la información es demorada para realizar sus tareas y análisis.

5. Cree usted que al no existir una red de datos entre la matriz y la sucursal influya en la gestión comercial de la empresa?

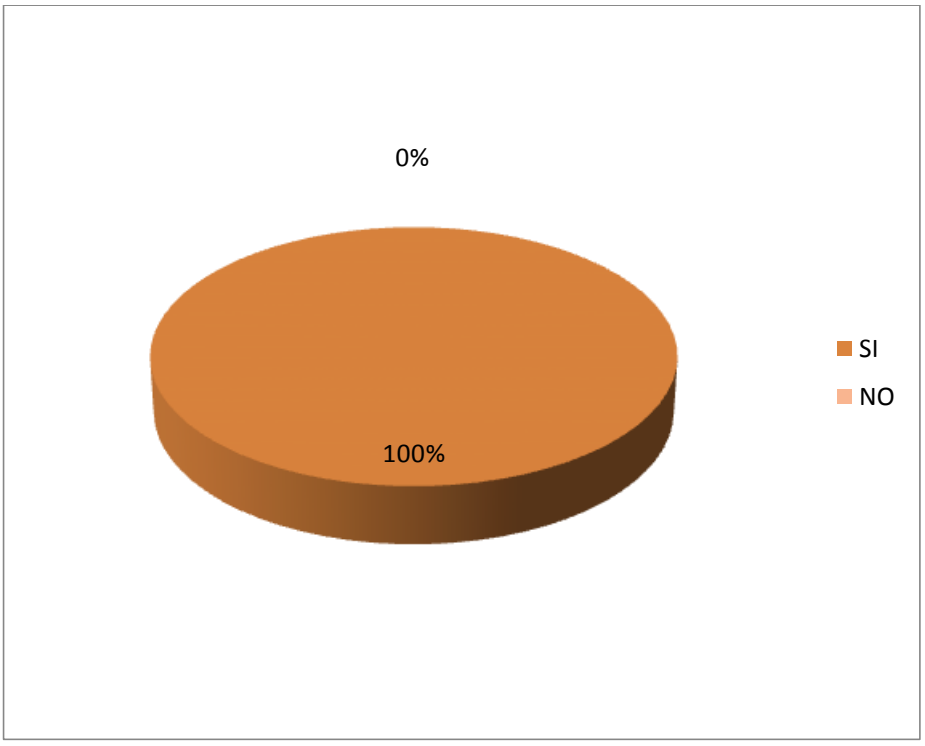
SI		NO	
%	Valor	%	Valor
92	9	8	1



El noventa y dos por ciento del personal indica que si influye en la gestión comercial el no tener una red de datos entre la matriz y la sucursal.

6. Considera usted necesario la instalación de un sistema de comunicaciones inalámbricas que permita la consolidación de la información de todos sus centros de manera centralizada y oportuna?

SI		NO	
%	Valor	%	Valor
100	10	0	0



Es necesario aplicar un sistema de comunicaciones que nos permita integrar todos los centros y agencias para consolidación de la información, existe un cien por ciento que está de acuerdo.

3.6 VERIFICACIÓN DE LA HIPÓTESIS

Para la demostración de la hipótesis empezaremos recordándola: “Con la implementación de una red man se mejorará la gestión de ventas”.

Luego de que el sistema de comunicaciones ha sido implementado vamos demostrar nuestra hipótesis en base a la comparación de la gestión comercial antes del sistema y hoy con el sistema de comunicación. El proceso comparativo se basa en recoger las opiniones del personal administrativo, para su evaluación, se procede a realizar las siguientes preguntas:

- ¿Con la implementación del Sistema de comunicaciones la información a permitido mejorar el proceso de ventas?
- ¿Se puede compartir información entre los centros y Agencias y realizar estadísticas acertadas?
- ¿El sistema de comunicación inalámbrica permite compartir recursos y disminuye los costos operativos?

Mediante la encuesta realizada a los clientes internos, se obtuvo los siguientes datos:

SI			NO		
%	Nº	Valor	%	Nº	Valor
100	1	10	0	1	0
	2	10		2	0
	3	10		3	0

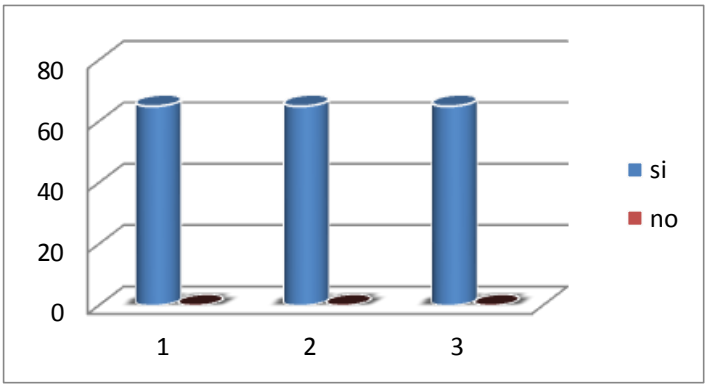


Grafico: 7 Verificación de hipótesis

De los resultados anteriores se puede claramente apreciar que la gestión comercial se verá notablemente apoyada por la información generada en la agencia y transmitidas instantáneamente a la matriz, esta información actualizada ha permitido realizar ventas y tomar decisiones eficientes y sobre todo muy a tiempo. De esto podemos concluir además que con el sistema de comunicaciones inalámbrico se mejorará la gestión comercial y es lo que queríamos demostrar.

3.7 CONCLUSIONES

En base a las encuestas realizadas a los clientes internos de la empresa determinamos:

- La empresa comparte y actualiza información manualmente interna y externamente
- Hay retraso en llegar la información de la agencia a la matriz
- La información no es confiable por la demora
- La empresa muchas veces no vende por no tener actualizado su inventario.
- La emisión de informes de ventas es demorado

3.8 RECOMENDACIONES

- Instalar una Red Wireless de tipo MAN que una la agencia con la matriz.
- Capacitar el personal en el manejo de la red Híbrida
- Automatizar procesos de control administrativos
- Actualizar equipos de computación

CAPITULO IV

MARCO PROPOSITIVO

4.1 TEMA

Diseño de una red Híbrida para la Gestión de Ventas de la Empresa Mora e hijos de la ciudad de Babahoyo

4.2 INTRODUCCIÓN.

Una de las tecnologías más prometedoras y discutidas en esta década es el poder comunicar computadoras mediante tecnología inalámbrica, usando equipos de comunicaciones de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está, siendo ampliamente investigado. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos, gracias a los equipos Dlink 3200ap esto ya es posible.

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. 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 WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red inalámbrica, 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 ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (hot spots) en las próximas redes de tercera generación (3G) se ven como las aplicaciones de más interés durante los próximos años.

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como son los PDAs (Personal Digital Assistants), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

4.3 OBJETIVOS DE LA PROPUESTA

4.3.1 GENERAL.

Mejorar la gestión de ventas de la empresa Mora e hijos en base a la implementación de una red Híbrida diseñada en esta tesis.

4.3.2 ESPECÍFICOS.

- Diseñar la red Híbrida que une la matriz con la fábrica y con la sucursal.
- Diseñar un sistema de comunicación de datos al interior de la matriz y de sucursal, esto quiere decir hacer una red LAN alámbrica e inalámbrica al interior de la matriz y de la sucursal.

4.4 DESCRIPCIÓN DE LA PROPUESTA

La propuesta de solución al problema planteado en el Capítulo I, consiste en la **implementación de una Red Híbrida**, la misma que permitirá compartir información entre las dos dependencias de la Empresa, y entre los departamentos o secciones de la matriz y de la sucursal, se espera que con este recurso tecnológico se pueda lograr un mejoramiento de la gestión comercial de la empresa

Ahora de manera general, se puede señalar que lo que se va a implementar es la red de toda la empresa, ya que actualmente no existe ninguna red en ella, esto

quiere decir que se instalará una red LAN para el interior de cada dependencia, la misma que será de tipo hibrida ya que los PC de escritorio estarán conectadas mediante cable utp categoría 6, mientras que las portátiles pueden hacerlo inalámbricamente. Tanto la sucursal como la matriz estarán enlazadas mediante la red Híbrida formada por radios con antena incorporada. La red que se diseñe debe contemplar la posibilidad de incorporar nuevas tecnologías y nuevos servicios como voz sobre IP, video, etc. A continuación un esquema general de la red propuesta.

4.5. DESARROLLO DE LA PROPUESTA.

La implementación de la red mixta dependerá exclusivamente de la empresa pero a continuación procedemos a realizar el diseño de la misma de tal manera que la compañía se base en él para tomar una decisión positiva para la implementación.

4.5.1 ANÁLISIS PREVIO.

Para comenzar el diseño de la red inicialmente detallaremos las ubicaciones de los equipos así como de las sucursales. Analizaremos las distancias entre las mismas para que en base a ello se pueda definir por los dispositivos.

Como mencionamos en el capítulo inicial la empresa Mora e hijos se dedica a la producción y comercialización de plantas para zapatos y material de zapatería en general, dispone de dos puntos de ventas ubicados aproximadamente a 200

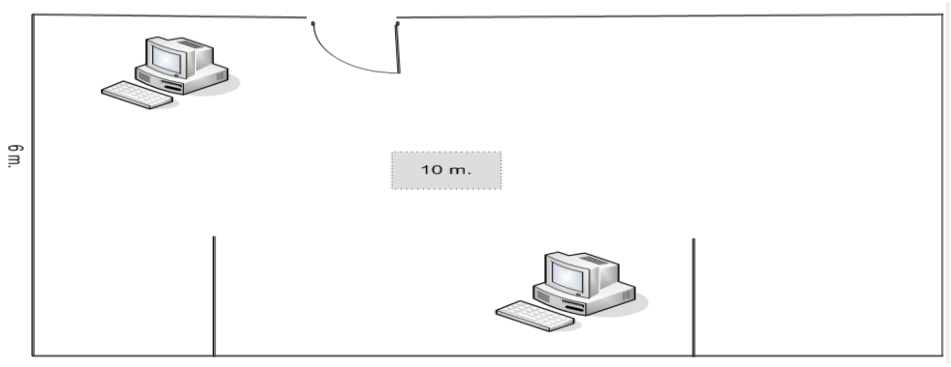
metros. En el primer punto de venta se lo podría considerar como matriz ya que se tiene el almacén, la bodega y en el piso superior disponemos de las oficinas administrativas, esta se halla en las calles Pedro Carbo entre 10 de Agosto y 5 de Junio . En el otro sitio de venta tan solo se dispone del almacén con los productos a venderse y su dirección es General Barona entre Rocafuerte y Eloy Alfaro.

A más de ello la pequeña fábrica que produce las plantas se halla ubicada en la ciudad de Bario Lindo sector la Maternidad aproximadamente a 900 m. de distancia.

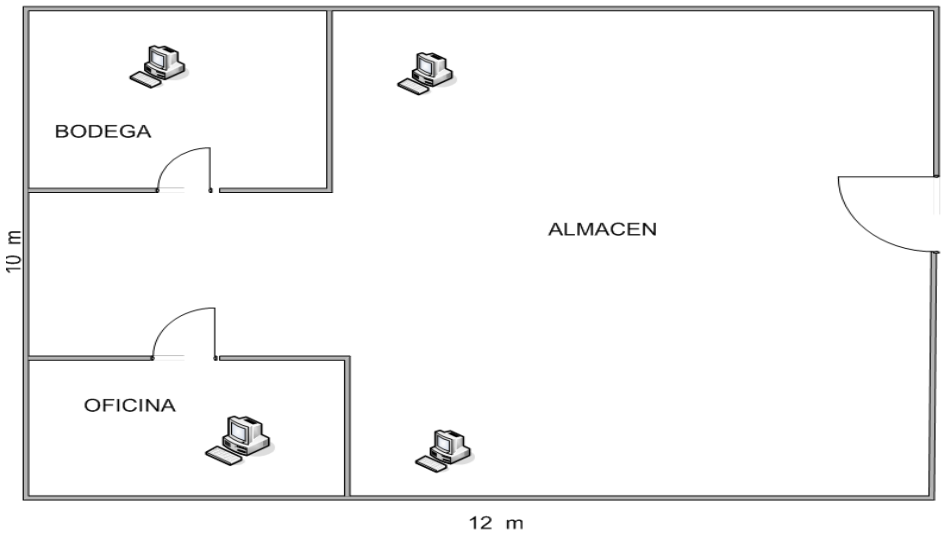
Actualmente en la sucursal se dispone de dos computadoras sin ningún medio de enlace, en la matriz en cambio se tiene cuatro computadoras para el uso de bodega y del almacén, de igual manera en la sección administrativa disponemos de cuatro computadoras utilizadas por el Gerente, el Contador y las secretarias. Se debe mencionar que existe una apertura total por parte del Gerente hacia lo que es sistematización y redes informáticas dentro de la empresa, eso quiere decir que la empresa piensa ampliar el número de computadoras que poseen lo cual implica que deberemos tomar en cuenta dicho criterio para nuestro diseño.

A continuación ponemos los gráficos respectivos de los almacenes y la ubicación actual de las computadoras en los mismos.

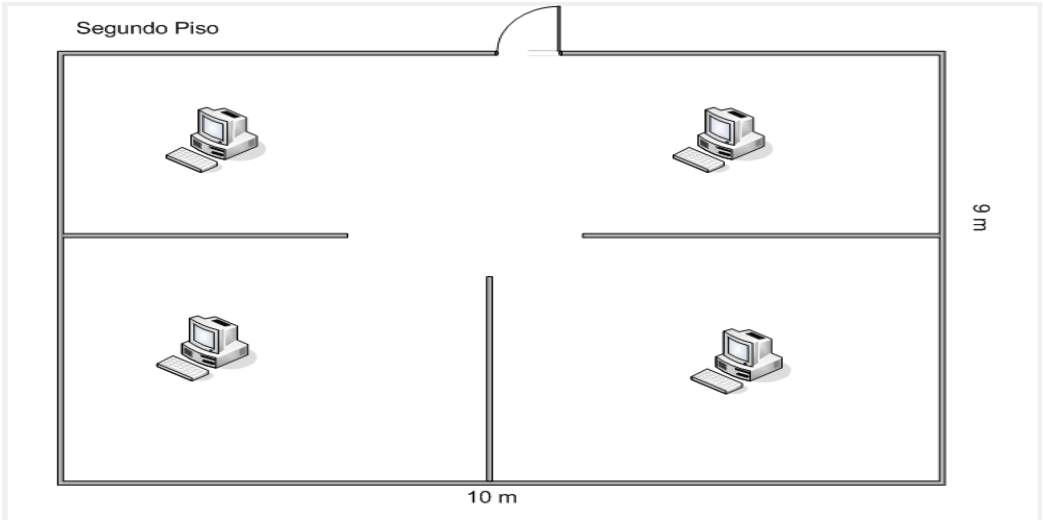
Sucursal:



Matriz: almacén y oficinas administrativas



Oficinas Administrativas.



En la fábrica existe tan solo un computador por lo que no amerita realizar el gráfico de la ubicación. Se puede deducir que primeramente deberá enlazarse los equipos dentro de los almacenes y en el interior de las oficinas administrativas, cabe recordar que las oficinas administrativas se encuentran en el messanine superior del piso. En cuanto a los equipos estos poseen las siguientes características:

- Sucursal

No.	Modelo	Memoria	Tarjeta Red	USB	Disco Duro
01	Pentium IV	128	Si	Si	**20 Gigas**
02	**Pentium IV**	**256**	**Si**	**Si**	**40 Gigas**

- Matriz

No.	Modelo	Memoria	Tarjeta Red	USB	Disco Duro
03	Pentium IV	256	Si	No	**20 Gigas**
04	Pentium IV	128	SI	No	**20 Gigas**
05	Pentium IV	256	SI	SI	**80 Gigas**
06	**Pentium IV**	**256**	**SI**	**SI**	**80 Gigas**

- Administrativas.

No.	Modelo	Memoria	Tarjeta Red	USB	Disco Duro
07	Pentium IV	128	Si	Si	**20 Gigas**
08	Pentium IV	128	SI	si	**20 Gigas**
09	Pentium IV	256	SI	SI	**80 Gigas**
10	**Pentium IV**	**256**	**SI**	**SI**	**80 Gigas**

Del cuadro de las características de los equipos se puede apreciar que todos poseen tarjeta de red y pórtico USB. Debido a estas características se recomienda que el enlace dentro de los almacenes y las oficinas sean mediante cable UTP. Se prevé también que la comunicación entre la oficina administrativa y el almacén en la matriz sea mediante un Router-Access point, quedando para enlazar la matriz con la sucursal mediante radio Access point que incorpora una antena, estos generalmente tienen capacidades de hasta 5km en su alcance.

4.5.2 DISEÑO

El diseño de una red debe estar basado en las actividades comunes que realiza la misma, debe ser elaborada con estándares y especificaciones adecuadas, de tal manera que incluso pueda soportar nuevas tecnologías

4.5.2.1. Definición de nuevas exigencias de la red creada.

Esencialmente el objetivo de esta etapa, es definir las especificaciones para cumplir con los objetivos y estándares de la nueva red. En primera instancia se trata de analizar las perspectivas a corto y largo plazo de la compañía, al tiempo que se consideran los contratiempos. La justa definición de las exigencias implica siempre un análisis de perspectivas a corto y largo plazo en la empresa. Hay que garantizar que la red no se vuelva obsoleta con el paso del tiempo.

En base a estas premisas, se han definido las exigencias para la red de la empresa Mora e hijos.

4.5.2.2. Perspectiva a corto y largo plazo.

Partiremos del objetivo que tiene la empresa al implementar la red, este objetivo de manera general manifiesta que la empresa desea tener una comunicación de datos entre los diferentes departamento que hay en la matriz, así como entre las dependencias. Cada día se hace más necesaria, la comunicación entre matriz y sucursal, ya que a cada instante se requiere compartir la información existente en la bodega principal de la empresa, esto debido a que desde la sucursal se tiene que estar llamando por teléfono para averiguar si existe tal o cual producto. Estas consultas telefónicas producen demora en el servicio, lo cual generalmente molesta a los clientes y a menudo por ello se pierde la venta respectiva.

Con una red de datos entre departamentos y sucursales se puede compartir información sobre el inventario existente, esto permitirá acelerador el proceso de atención al usuario y muy probablemente elevar las ventas. Hay que mencionar también que, la empresa está en un proceso de expansión, lo cual implica que está planificado abrir nuevas sucursales en la ciudad y también ampliar las ya existentes. Esto significa que la red deberá tener la capacidad de ampliarse, es decir disponer de más sitios de conexión a nivel local y a nivel metropolitano.

Esto quiere decir especialmente que, la red man debe estar en capacidad de ampliarse a nuevos sitios dentro de la ciudad de Babahoyo y al interior de cada dependencia deberá poderse conectar mas computadores.

4.5.2.3. Nuevos Servicios y tecnologías.

La red híbrida deberá permitir disponer de nuevos **servicios como INTERNET** en todas las dependencias, correo electrónico Interno, mensajería instantánea en todas las dependencias, a más del principal que era compartir información.

Con la red habilitada, las **ventas podrán ser canceladas** ya no solo de contado sino también con tarjeta de crédito. Es decir que, es el cliente el beneficiado directo de la instalación de la red Híbrida en la empresa. Como nuevas tecnologías a futuro se puede señalar que la empresa podría contar con un **servicio telefónico de voz sobre IP**, lo cual permitiría lograr un ahorro en la comunicación telefónica al interior de la empresa.

También mediante la red, se puede hacer **monitoreo de vigilancia con cámaras** para cada dependencia, esto significaría mejorar la seguridad de los locales, así como de los clientes que llegan a los mismos.

4.5.2.4. Tiempo de respuesta.

La red esencialmente permite compartir información entre dependencias y sucursales a través de los sistemas de inventario y facturación, a mas de ello debe responder a las exigencias de trafico de 10 Mega Bits actualmente a 100 Megabits próximamente.

El tiempo de respuesta, es una variable importante que se analiza en el proceso de diseño de la una red, para nuestro caso de estudio, lo hemos calculado en base a la siguiente fórmula:

TR = TME + TTA + TMS

Donde:

TR.- Es el tiempo de respuesta al interior de la red.

TME.- Tiempo del mensaje al entrar, esta duración comprende el tiempo de transmisión y el tiempo en la fila de espera de un controlador inteligente. Una duración típica del tiempo del mensaje al ingresar es de 0,6 segundos.

TTA.- Tiempo de procesamiento de la aplicación, esta duración incluye el tiempo del procesamiento del programa y todos los tiempos de acceso a la base de datos. Una duración típica del TTA es de 0,5 segundos.

TMS.- Tiempo del mensaje al salir, esta duración comprende el tiempo de espera en una fila a la salida d la computadora o de cualquier otro dispositivo de transmisión remota. Una duración típica de TMS es de 0,7 segundos.

Tomando estos valores promedio referidos especialmente a transacciones podemos aplicarlos en la formula, teniendo:

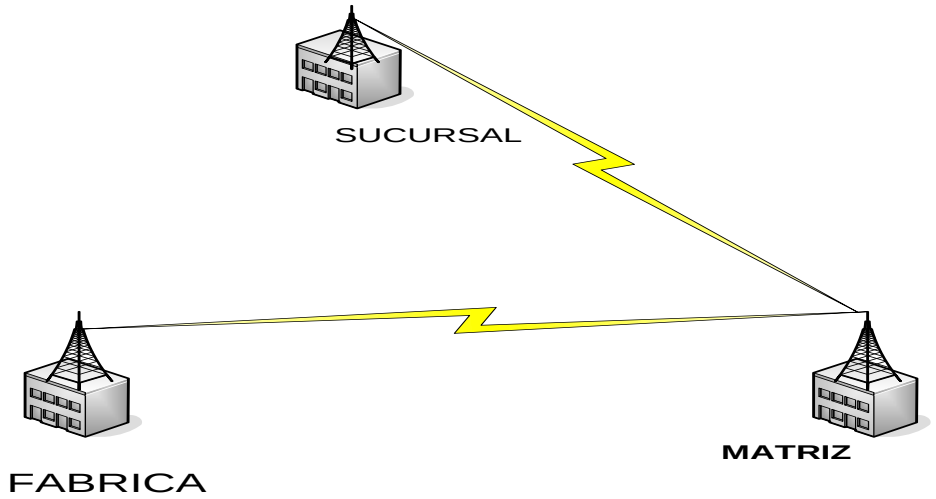
TR = 0,6 + 0,5 + 0,7 = 1,8 segundos

Eso significa que por nuestra red, deberemos realizar transacciones que van a durar menos de 2 segundos en ser respondidas. Hay que tomar en cuenta que existen factores en una red man que demoran este tiempo de respuesta. Esos factores, tienen que ver con velocidad de dispositivos de almacenamiento y acceso a bases de datos, así como los de comunicaciones e incluso el clima en ese momento, ya que puede producir interferencia porque hay que recordar que nuestra idea es enlazar la empresa mediante antenas..

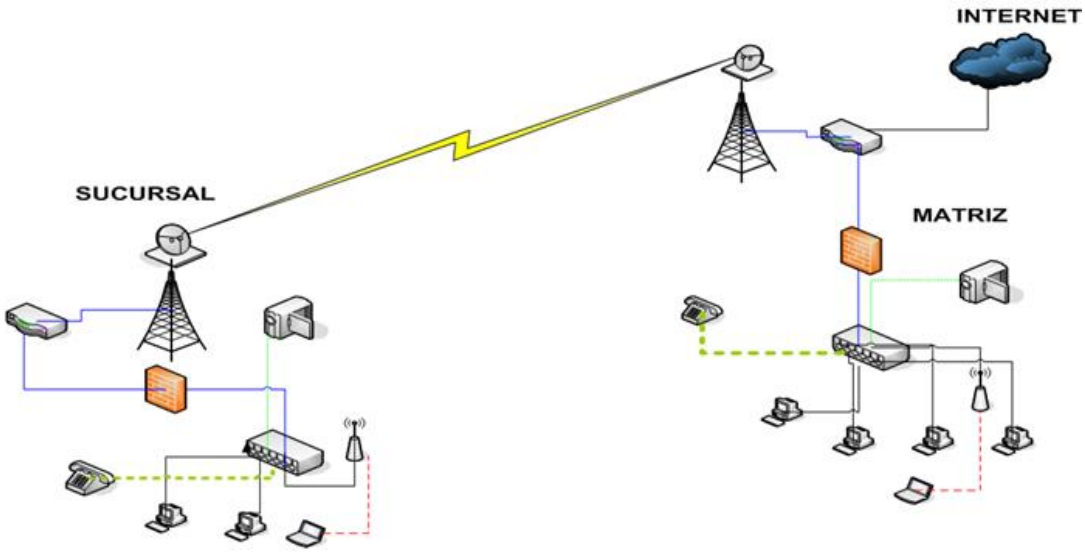
En caso de aplicar un ping en nuestra red, la demora no debe ser mayor a 180 mili segundos.

4.5.2.6 Diseño general de la red Híbrida.

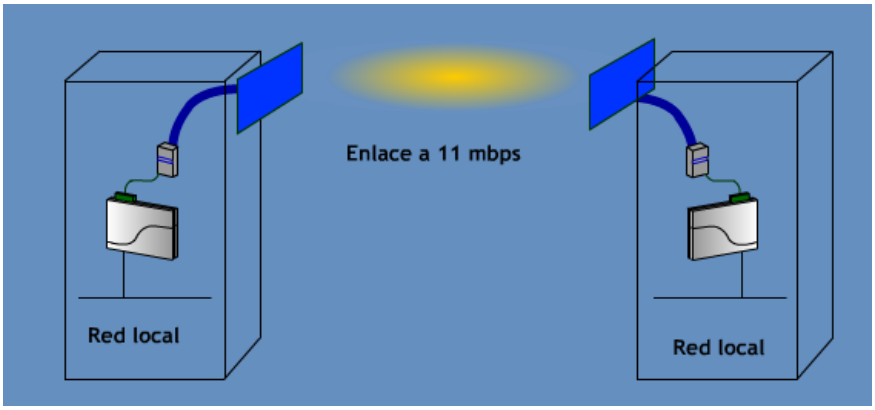
Seguidamente ilustramos el enlace entre la sucursal, la matriz y la fábrica.



A continuación una estructuración general del enlace matriz-sucursal, con las respectivas redes internas, a más de ello un bosquejo con los posibles futuros servicios a incorporar en la red.

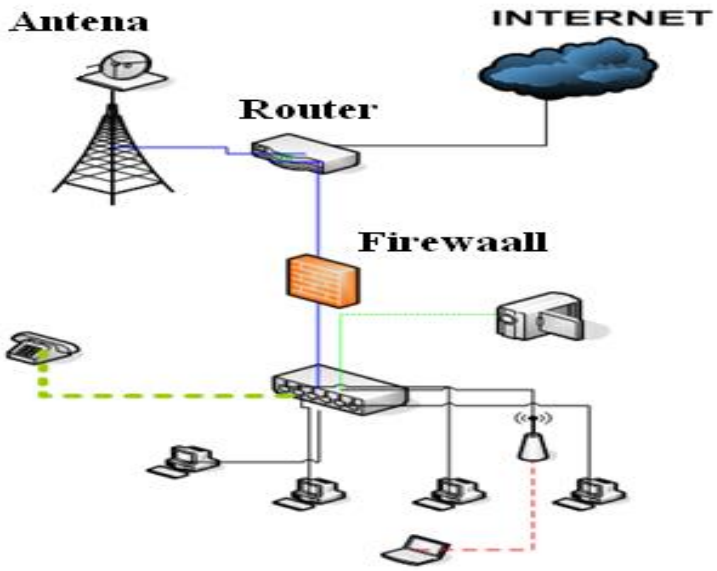


El enlace consiste en realizar una red punto a punto con la siguiente estructura general



El enlace punto a punto proporciona soluciones de conectividad para empresas con centros de trabajo múltiples que necesiten de una gran coordinación y trabajo compartido. Este enlace proporciona a la empresa un entorno de intercambio de información con un coste periódico de cero, tan sólo la información. Es el complemento exterior perfecto a una instalación interior de red local estándar o inalámbrica. Efectivamente, todos los centros conectados por el enlace punto a punto formarán parte de una única red local, exactamente como si estuvieran en el mismo edificio, pero con la flexibilidad que proporciona la distribución multicentro, imprescindible en el entorno empresarial cambiante de hoy en día.

Gracias a la potente antena o parrilla de emisión / recepción, que utiliza un protocolo similar al de la red local inalámbrica, pero con un alcance extendido; pueden unirse mediante el enlace punto a punto centros situados hasta a 15 kilómetros. El enlace general, es detallado en el diagrama global de la red, del mismo que se toma la parte relacionada con la matriz y nos queda el siguiente esquema mas especifico.



De este diagrama se deduce que se requiere de los siguientes elementos para el enlace:

DISPOSITIVO	IMAGEN	PRECIO
3 Router TRENDNET de 4 puertos, printserver USB TW100-BRF114U + Firewall **Incluye FIREWALL** **Pórtico USB para impresora**		**600**

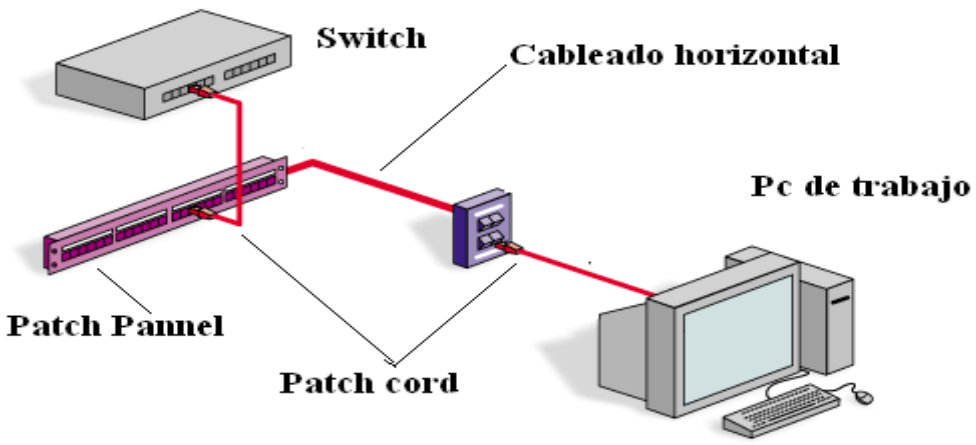
3 Puntos de Acceso Inalámbrico (Access Point) T**RENDNET 54Mbps TL-WA5210G.** **Con antena incorporada.** **En modo inalámbrico tiene rangos de hasta 15 Km.** **De instalación externa**		**900**
Cable coaxil 50 M, conectores macho-hembra, tubos para torres (antenas) y extras		**250**
	TOTAL	**1750**

Cabe señalar que se tiene línea de vista entre la matriz y la fábrica, ya que la misma se encuentra en una parte alta de la ciudad. Por otro lado, entre la matriz y la sucursal para poder tener total línea de vista, los radios access point m van sujetos en armazones con tubos que forman torres de aproximadamente 10 m. de altura. Luego de tener los elementos se procede al direccionamiento de los mismos.

LUGAR	DISPOSITIVO	Dirección	Mascara	Pta. enlace
MATRIZ				
	ROUTER1	192.168.10.99	255.255.255.0	
	RE1	192.168.10.91	255.255.255.0	192.168.10.99
FABRICA	ROUTER2	192.168.10.96	255.255.255.0	192.168.10.98
	RE2	192.168.10.98	255.255.255.0	192.168.10.99
SUCURSAL				
	ROUTER2	192.168.10.93	255.255.255.0	192.168.10.95
	RE2	192.168.10.95	255.255.255.0	192.168.10.99

4.5.2.7 Diseño de la red LAN (Matriz y sucursal)

Según lo manifestado en el análisis previo el enlace de las computadoras en el interior de los almacenes y la oficina administrativa podrá quedar de la siguiente manera: Se tendrá un cableado estructurado con cable **UTP categoría 6**, en este caso el cableado solo será el de tipo horizontal.



- La norma aplicada en este cableado horizontal es la ANSI/TIA/EIA 568A.
- La topología de red será en estrella.
- No se permiten cables con longitudes mayores a 90 m.
- Se utilizarán conectores RJ45, con cable utp categoría 6 para que la red soporte altas velocidades (hasta 300 Mbps)
- Se utilizará un patch panel Lanpro de 16 pórticos y un swicth 3Com de igual número de puertos. Como solo hay un patch panel y un switch se utilizara un rack de pared.

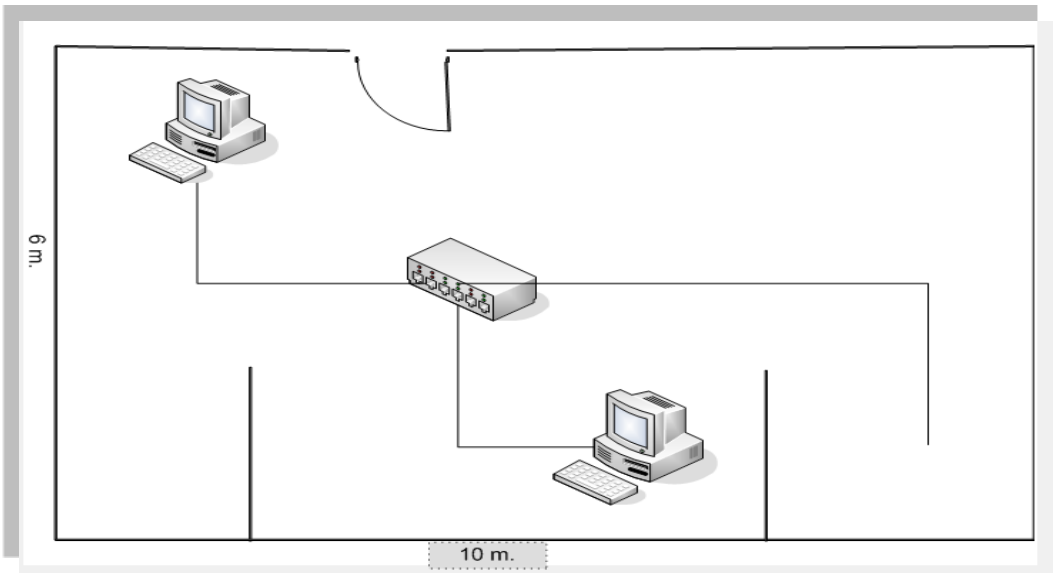
Además se abre la posibilidad de que se tenga una **red inalámbrica** al interior de cada local, para ello se instalará un Access point Dlink Ap 2100 que es un elemento inalámbrico de alto rendimiento. Para la fábrica, internamente se hará una red inalámbrica, para ello se incorpora un adaptador de red inalámbrico USB al equipo existente. El direccionamiento será:

LUGAR	No de Pc.	Dirección	Mascara	Pta. enlace
MATRIZ	**1**	**192.168.10.10**	**255.255.255.0**	**192.168.10.99**
	2	**192.168.10.11**	**255.255.255.0**	**192.168.10.99**
	3	**192.168.10.12**	**255.255.255.0**	**192.168.10.99**
	4	**192.168.10.13**	**255.255.255.0**	**192.168.10.99**
	5	**192.168.10.16**	**255.255.255.0**	**192.168.10.99**
	6	**192.168.10.17**	**255.255.255.0**	**192.168.10.99**
	7	**192.168.10.18**	**255.255.255.0**	**192.168.10.99**

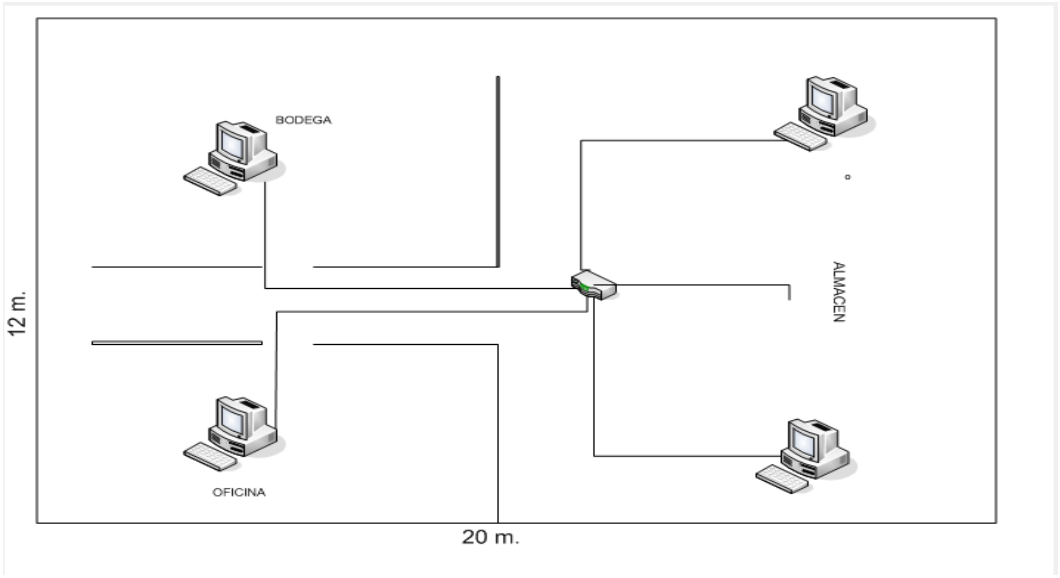
	8	**192.168.10.19**	**255.255.255.0**	**192.168.10.99**
	AP1	**192.169.10.25**	**255.255.255.0**	**192.168.10.99**
FABRICA	**1**	**192.168.10.41**	**255.255.255.0**	**192.168.10.96**
	AP3	**192.169.10.45**	**255.255.255.0**	**192.168.10.96**
SUCURSAL				
	1	**192.168.10.31**	**255.255.255.0**	**192.168.10.93**
	2	**192.168.10.32**	**255.255.255.0**	**192.168.10.93**
	AP2	**192.168.10.45**	**255.255.255.0**	**192.168.10.93**

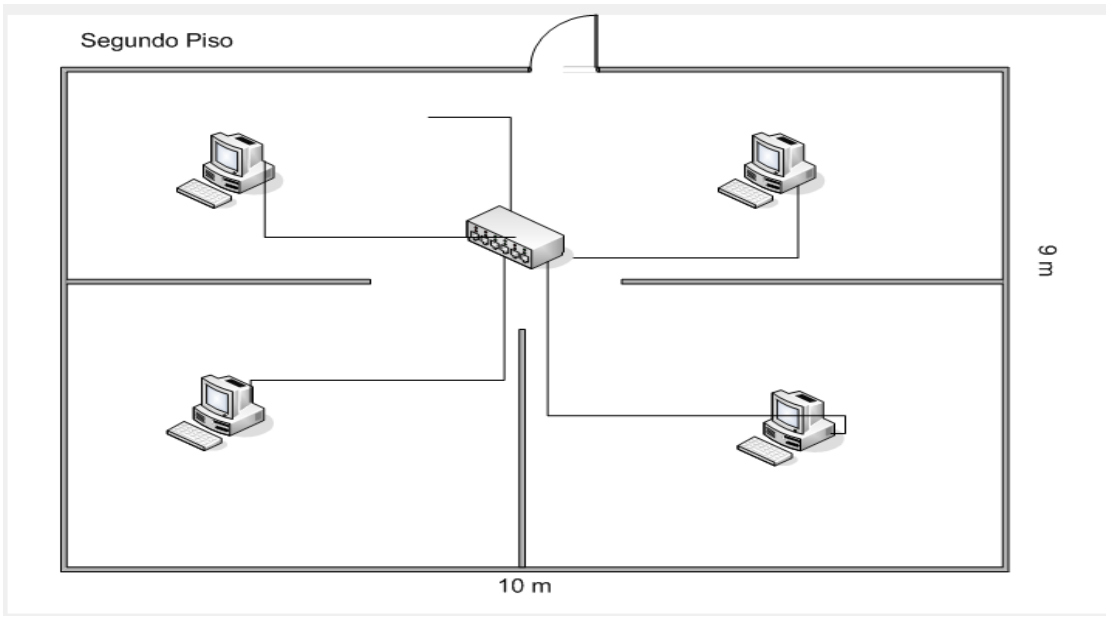
Esquemáticamente nos quedaría:

Sucursal:



Matriz, almacén y oficinas administrativas





De los gráficos anteriores podemos señalar que se necesitan los siguientes materiales para el cableado horizontal, con los precios respectivos:

Cant.	Material	Pre. Uni.	Total
2	Switch 3COM - 3C16792 - 16-Port 10/100Mbps Office Connect Dual Speed Network Switch	60.00	**120.0**
100 m	Cable utp nexxt cat.6	0.50	**50.0**
30	Conector rj45 cat.6	0.33	**10.0**
3	Acess point Dlink AP2100	90	**270.0**
2	**Patch Panel 16 Puertos Cat6 Lanpro**	60	**120.0**
2	Rack de pared desmontable	110	**220.0**
10	Toma de usuario (Placa, conector)	5	**50.0**
40 m	Canaletas.	1	**40.0**
	Extras (uniones, capuchones, tornillos, etc.) y adaptador USB inalambrico		**60.0**
TOTAL			**960.0**

4.5.2.8 Costo total de la red.

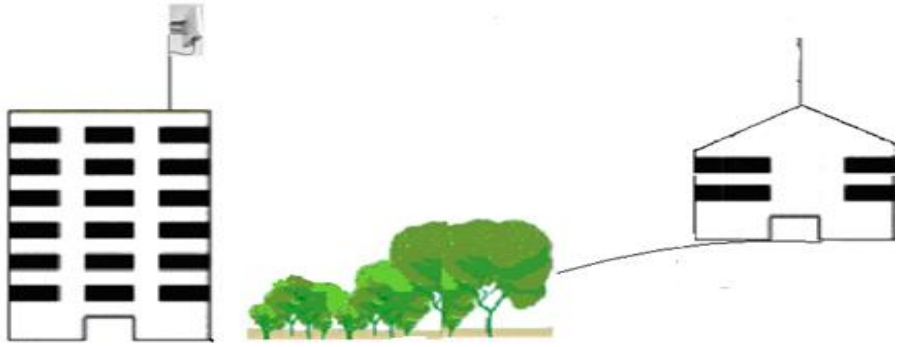
El valor total de la red será:

ESPECIFICACIÓN	VALOR
RED MAN	1750
RED LAN	960
EXTRAS	290
TOTAL	3000

4.5.3 IMPLEMENTACIÓN DE LA RED HÍBRIDA

4.5.3.1 Enlace Metropolitano

Primeramente se define las características de las dos torres, cada una de ellas tiene un tubo de 10 metros de altura, 1.5 pulgadas de grosor que serán ubicadas en las terrazas de los respectivos edificios. En el edificio de la matriz va la antena omnidireccional mientras que en la sucursal se coloca la otra antena, estas montadas sobre las estructuras metálicas, las mismas que permiten obtener una línea de vista perfecta entre los dos sitios. Las torres van empotradas en la terraza, ya que deben soportar las inclemencias del tiempo, no van pintadas pero si galvanizadas y con anticorrosivos.



Se procede a instalar las torres con las antenas respectivas y los radios externos, se utiliza el cable coaxial y los conectores macho y hembra respectivos. Los radios vienen con su estuche metálico que puede se sujetado en cualquier parte de terraza o de antena.

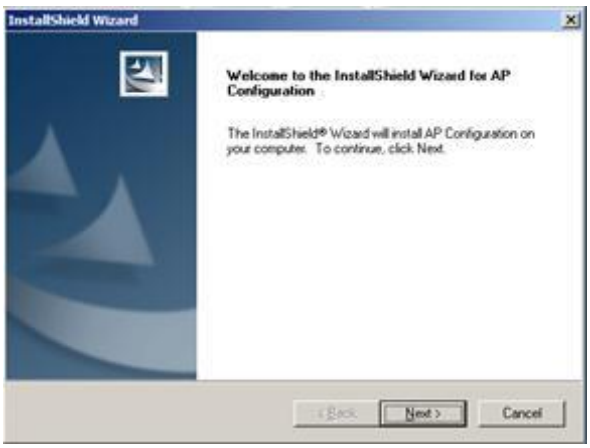
La conexión entre la antena y el radio es mediante cable coaxial con adaptador a utp. Se estima una distancia aproximada de 20 metros entre la antena, el radio externo, y el router, esta distancia es cubierta con cable utp categoría 6. Luego de la instalación física se procede a la instalación lógica.

Instalación del AP utilizando el CD.

- Presenta las siguientes ventanas

Pantalla de Inicio para configurar el AP

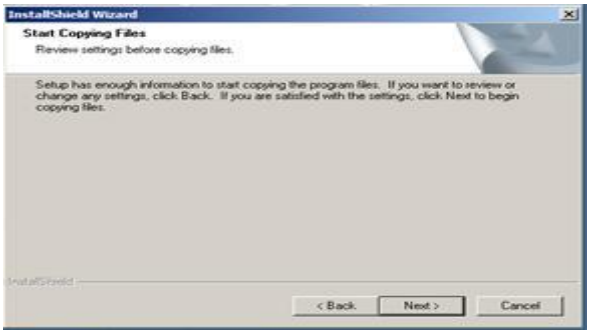
- Damos clic en next



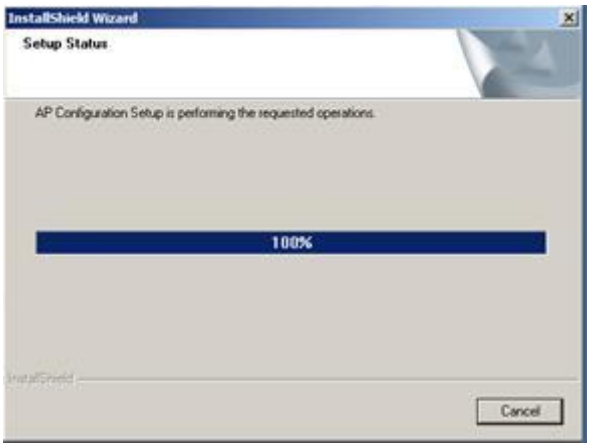
Pantalla de Bienvenida configuración AP

- Indicamos la dirección donde se va a instalar el software

- Damos clic en next



- Esta copiando en el disco todos los archivos que activaran el Access point para su configuración



- Damos clic en siguiente y luego finalizar

Luego de la Instalación del software nos vamos a **inicio, programas** y seleccionamos AP-Configuración en donde podemos buscar e identificar las conexiones con la dirección Ip, usuario y contraseña

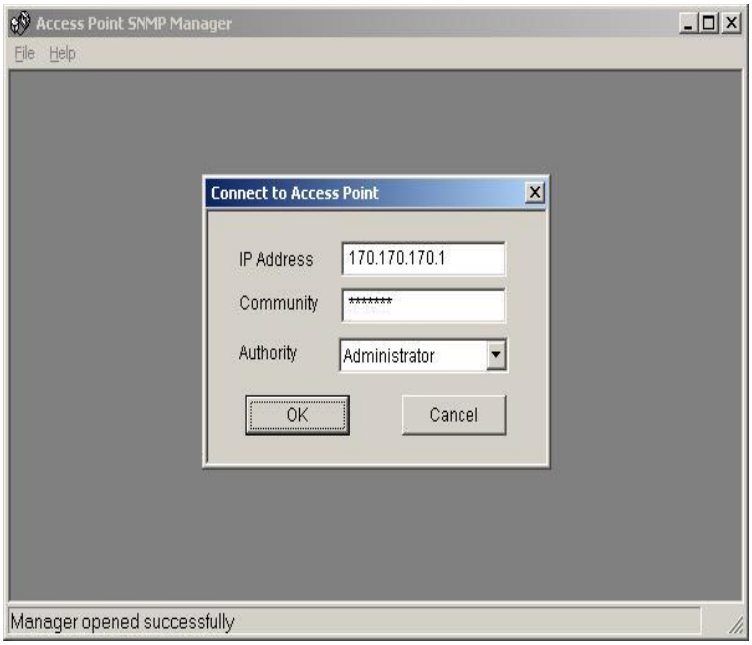
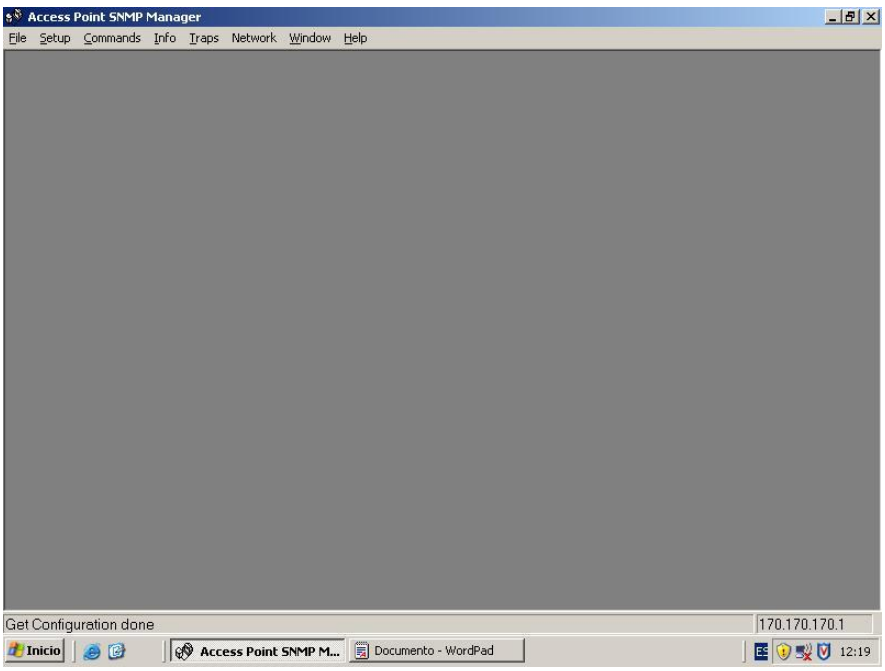
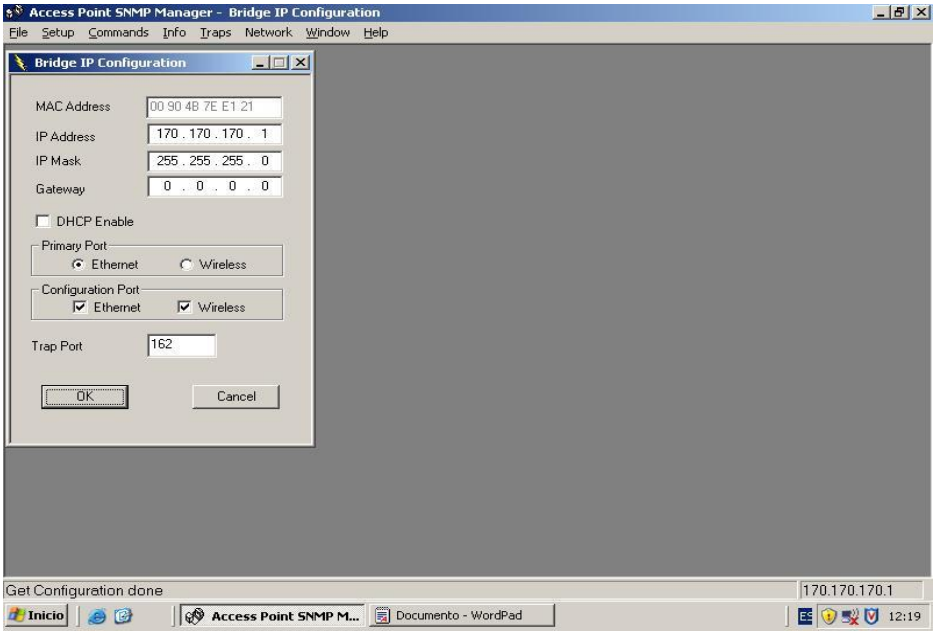


Grafico: 51 Pantalla de Acceso al AP

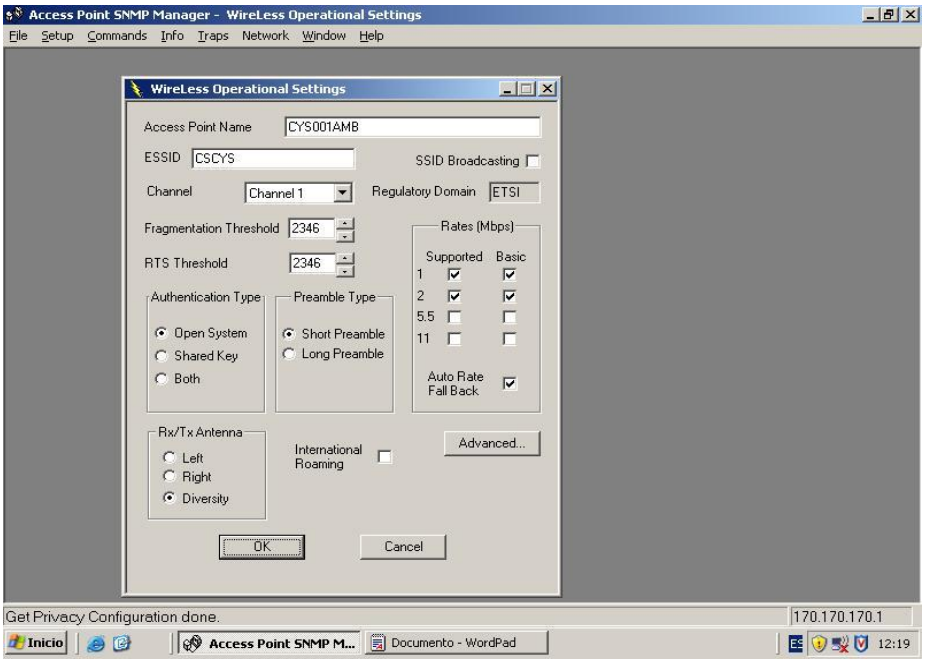
Nos muestra el Siguiente menú



En la opción setup del menú principal se selecciona para asignar la dirección ip de la conexión, dirección de MAC, la dirección de la máscara y el Gateway



Continuando con la configuración debemos asignar el nombre del acceso, nombre de la ID, tipo de conexión, antenas, etc.



Se define la MAC del cliente con el cual se establece la conexión

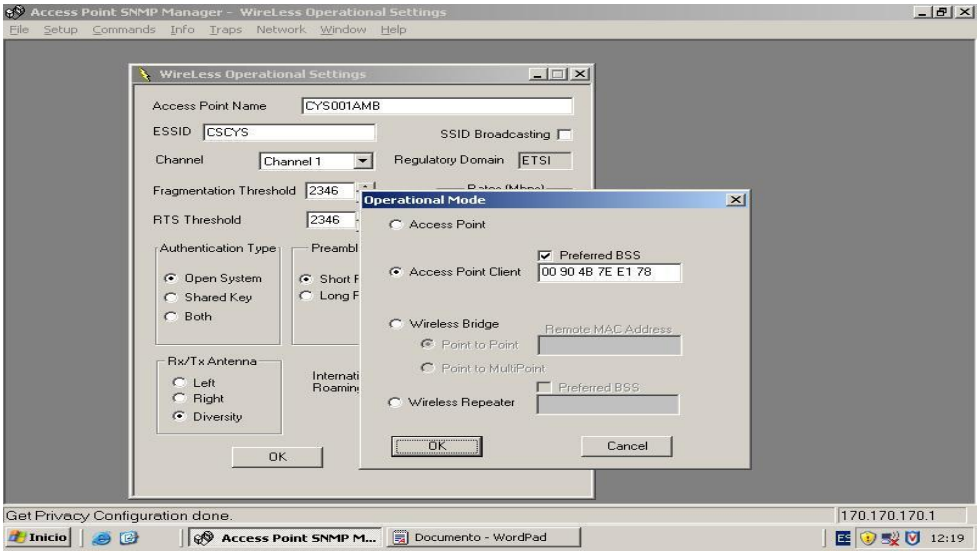
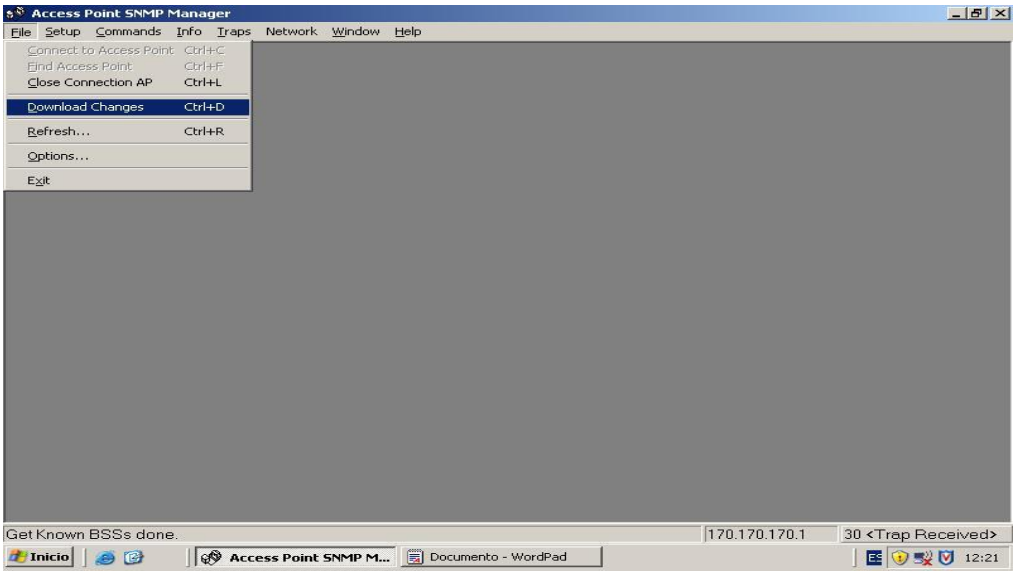


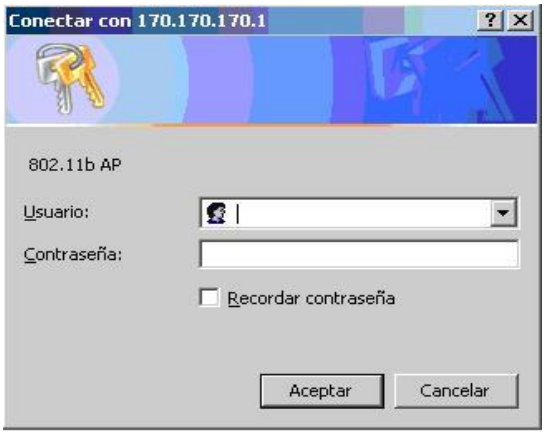
Grafico: 54 Pantalla del Mac Address del AP

Finalmente se graba los cambios realizados como muestra el gráfico la opción DOWNLOAD CHANGES

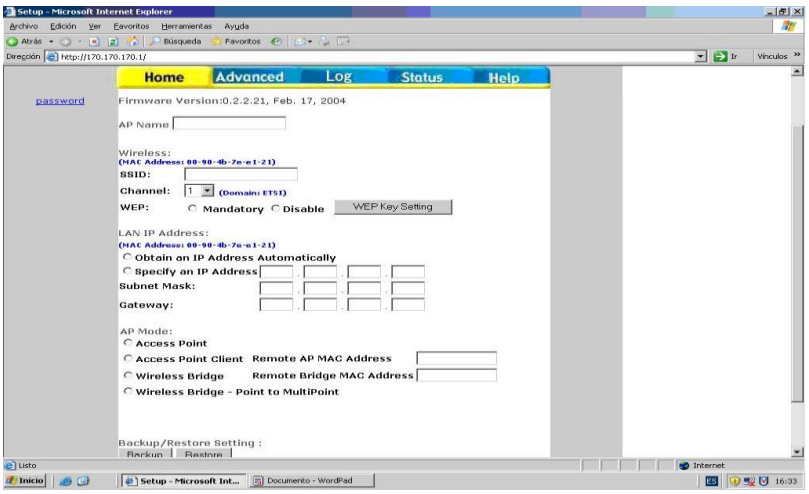


Instalación del AP Mediante WEB.

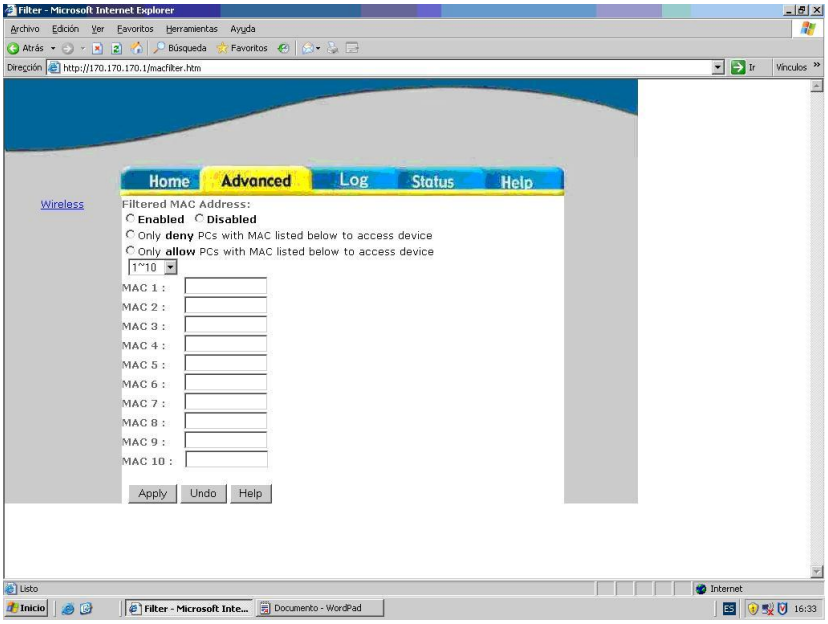
En la Instalación mediante Web colocamos la dirección, en nuestro caso 170.170.170.1 y nos presenta la siguiente ventana donde por defecto colocamos admin. Deje el espacio en blanco de la Contraseña. (Sin embargo, si se ha cambiado la contraseña, digitar la contraseña correcta.)



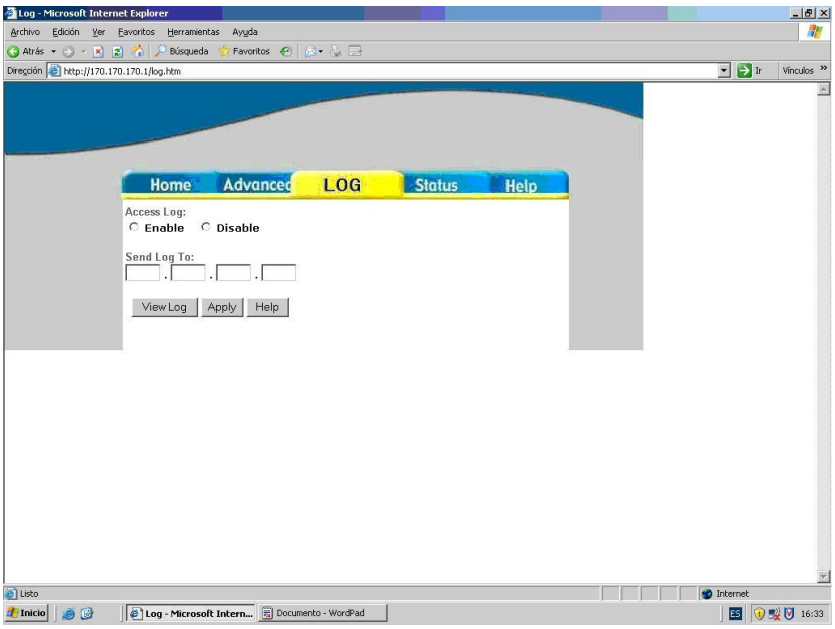
A continuación presenta la siguiente ventana, en esta ventana se debe definir el nombre de conexión, el nombre SSID, el canal de transmisión, indicar si se usara como access point.



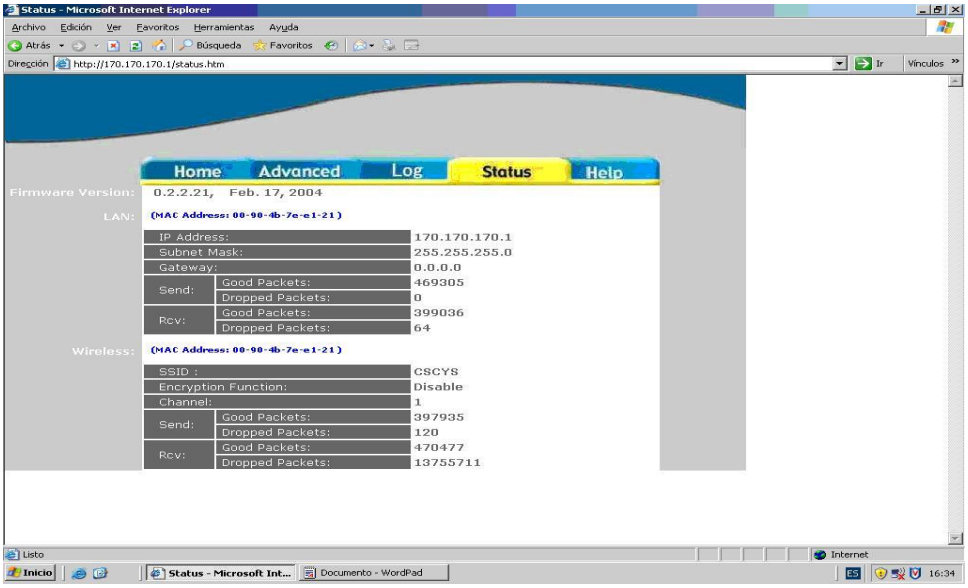
En esta ventana se indica la MAC Address del access point con la cual se realizará la conexión



Esta opción nos permite informarnos por acontecimientos que puedan ocurrir con la conexión la misma que enviara un mensaje a la dirección ip que se defina.



Finalmente esta ventana nos muestra la configuración realizada y el estatus de la conexión



La configuración del router es de forma similar al AP.

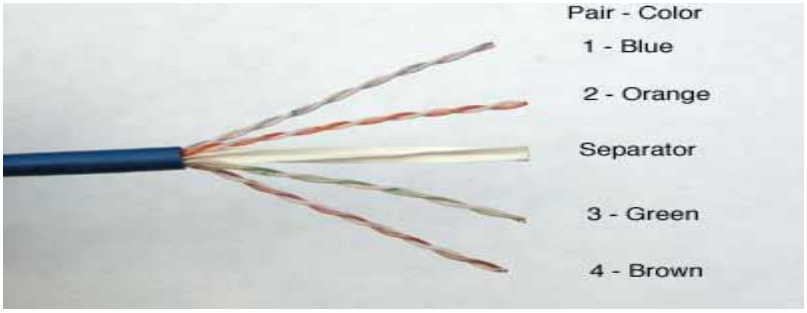
4.5.3.2 Instalación de la red LAN

La Categoría 6 actual de ISO/IEC y su correspondiente clase E nacieron en la histórica reunión de Munich en septiembre de 1997, donde se definieron los objetivos de ACR positivo a 200Mhz para categoría 6 y a 600 Mhz para categoría 7. Desde entonces la categoría 7 ha visto a menudo cuestionada su justificación y no ha tenido apenas desarrollo mientras que en Orlando (enero 1998) se añadieron parámetros adicionales para Categoría 6 y Categoría 5 Mejorada y en Tokio (mayo 1998) se definía la tabla de parámetros completa hasta 250 Mhz para Categoría 6.

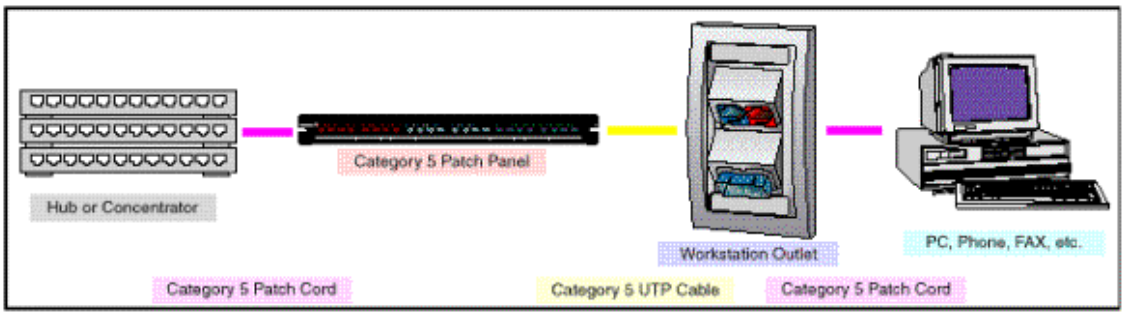
Los canales de Clase E, Categoría 6, operaran con conectividad RJ45 sobre sistemas de cableado UTP, FTP, o S-FTP y, en la definición del estándar, proveerán +ve PSACR a 200 Mhz. Ambas clases E y F ofrecerán rendimientos a efectos de información para frecuencias hasta un 25% por encima de los 200 y 600 Mhz, es decir, 250 y 750 Mhz, continuando con mismo razonamiento por el que se dará información hasta 125 Mhz en las clases D y D+.

Los estándares de Categoría 6 y Categoría 7 están siendo discutidos en los comités de estandarización. Así, Eurodatacab TC WG2 tiene borradores de propuestas sobre la Categoría 6 para ser entregados al CENELEC con rendimientos por encima de lo existente en Enero en ISO/IEC. ISO/IEC, por su lado, está actualmente discutiendo acerca del rendimiento requerido en el conector (la discusión principal está en la elección de 54 dB o 48 dB NEXT), y dependerá de la utilización o no de Cross Connect en el Canal, ya que el modelo básico del canal debe aún ser ratificado. EIA/TIA está también activamente trabajando en estas áreas. Hoy en día no existe un acuerdo en los rendimientos del enlace de Clase E, excepto en el claro objetivo de +ve PSACR a 200 Mhz e interconectividad RJ45.

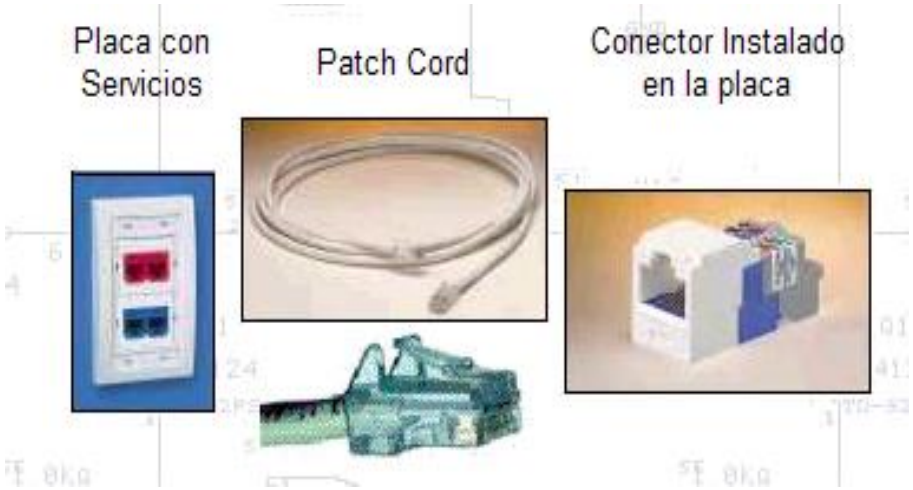
Ambos estándares de sistemas de cableado están siendo escritos en anticipación de las aplicaciones que requerirán dichos rendimientos, una situación similar a la que ocurrió con la definición de Categoría 5 en 1995. El cable que se ha decidido utilizar es de categoría 6, para trabajar con conectores rj45.



Inicialmente se debe conectar desde el área de trabajo al armario de conexión, a eso se denomina cableado horizontal, para ello se tiende la canaleta, se fijan las posiciones de las cajas conectoras y luego se poncha los cables respectivos. La estructura a lograr es la siguiente:

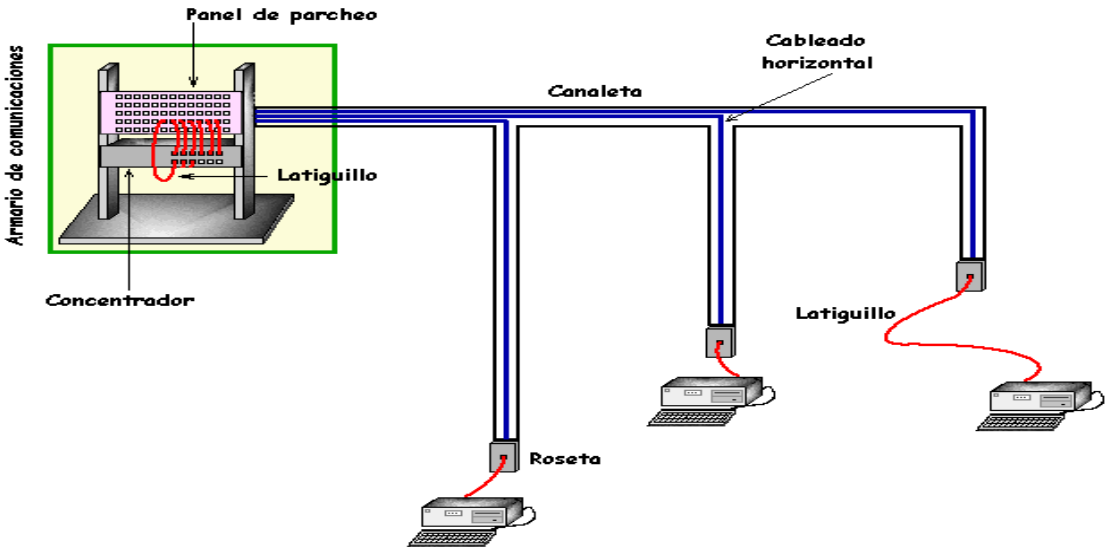


Para lograr esta estructura se utilizan los siguientes elementos:



La canaleta y las placas deberán quedar de la siguiente forma.

Finalmente la estructura a lograr es la siguiente:



En la parte física primeramente se tenderán los cables por las barrederas, se lo hará por el interior de las canaletas, los cables llegarán hasta el switch de cada piso y a los cajetines con los conectores rj45

Configuración de las PCS

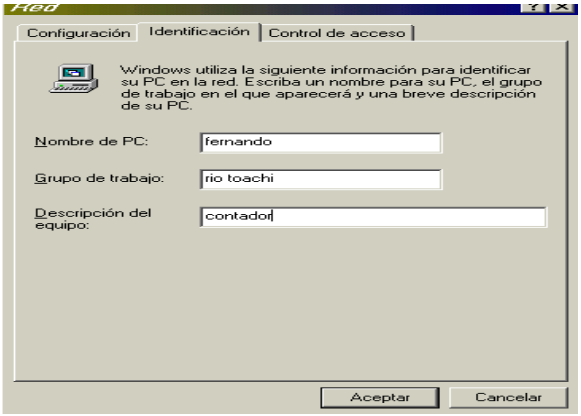
Para Configurar la dirección IP, nombre del equipo y grupo de trabajo hacemos lo siguiente:

Para la maquina uno y cuatro realizamos los siguientes pasos:

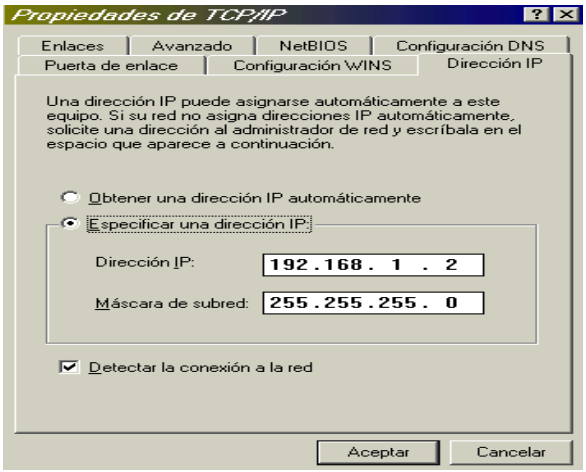
1.- Dar clic en **Entorno de Red** dentro del escritorio

2.- Seleccionar **Propiedades**

Propiedades >Identificación.- colocamos el nombre, Grupo de Trabajo y si deseamos la descripción del equipo.



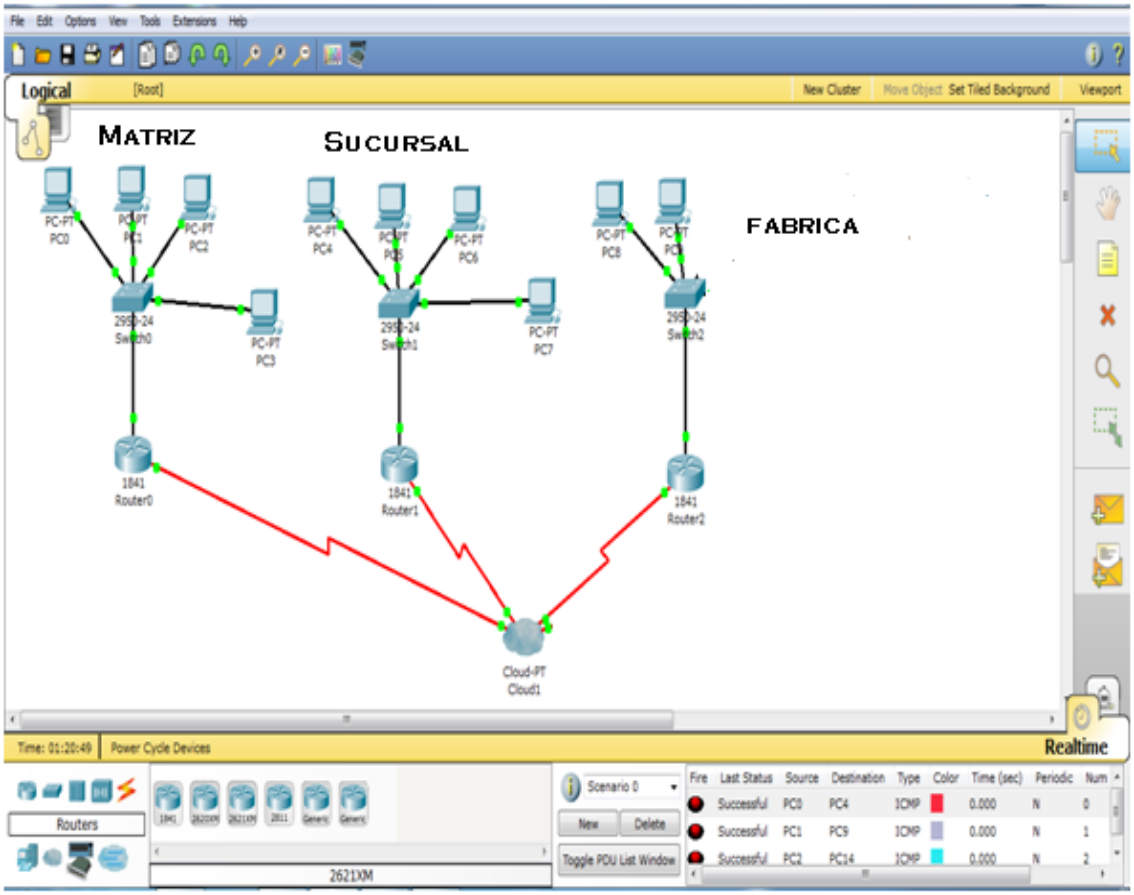
Propiedades > Configuración.- Dentro de las propiedades de TCP/IP especificamos la dirección IP y la máscara de subred.



3.- Aceptar, y reiniciar la pc.

4.5.3.3 Simulación de la red

El diseño lógico de la red se procedió realizarlo con el paquete computacional Packet Tracer de Cisco, para simular su correcto funcionamiento, quedando de la siguiente forma:



4.5.4 SEGURIDADES

La seguridad en las redes es de vital importancia para la supervivencia de la empresa, por lo tanto es primordial definir un plan de aseguramiento de la red y contar con una política de seguridad y confidencialidad para proteger los recursos de la red. A continuación hacemos un cuadro relacionador de los elementos de una red con los posibles riesgos que corre dicho elemento.

4.5.4.1. Gestión de seguridad de la red

El objetivo es asegurar la protección de la información en las redes y la protección de su infraestructura de soporte. Las redes deben controlase adecuadamente, a fin de estar protegidas de las amenazas, y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la informaciòn en trànsito.

Las caracterìsticas de seguridad, los niveles del servicio, y los requisitos de gestiòn de todos los servicios en red deben ser identificados e incluidos en los servicios de red, ya sea que estos servicios sean proporcionados en la instituciòn o subcontratados. La información manejada por los sistemas de información y las redes asociadas debe ser protegidas contra modificaciones no autorizadas, divulgación o destrucción. Se deben usar controles de acceso y claves para prevenir errores o negligencias del personal.

4.5.4.2 Uso de la Internet

Internet es una fuente de información valiosa pero también los virus que se adquieren a través de internet pueden dañar o eliminar archivos, o incluso borrar todo el disco duro, es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas. Se debe aplicar una política de seguridad y monitoreo constante. Además, mientras los usuarios están accediendo a información en Internet, terceras personas pueden estar observando los movimientos y la información de la empresa.

Por lo anterior, el responsable de seguridad desactivará la capacidad de los computadores para recibir archivos nocivos y evitará que los sitios Web registren los movimientos de los usuarios en Internet, por lo que se debe tener en cuenta lo siguiente:

4.5.4.3 Uso de Sitios web

El departamento de sistemas, supervisará e identificará, dentro de las categorías, los sitios web que más han sido visitados por los usuarios de la empresa, sobre pornografía, violencia, ocio, protectores de pantalla, gif animados, tarjetas electrónicas, música, videos y otros no relacionados con su trabajo y procederá a bloquear los sitios web y otros no relacionados con las funciones de la entidad.

4.5.4.4. Uso de Web Mail

No se otorgará accesos a Web mail no corporativos, como Hotmail, Yahoo, etc., en todo caso, podrá permitirse el acceso en casos extraordinarios por algún imprevisto o urgencia.

4.5.4.5. Uso de Messenger

El auge de la Mensajería Instantánea, le ha brindado nuevas oportunidades a los virus para que se propaguen y a los hackers para que accedan a su sistema.
Las amenazas a la mensajería instantánea son:

- Los gusanos y virus.
- Programas de puertas traseras o troyanos
- Secuestro de sesiones o suplantación de personalidad
- Denegación de servicio
- Divulgación de información no autorizada

Todos los programas de mensajería instantánea, envían las conversaciones sin cifrar, en texto plano, lo que no supone ningún problema para un hacker malicioso medianamente experimentado. Las sesiones no caducan y el programa abre la opción de recordar la clave, con lo que alguien con acceso a la máquina puede obtener información no sólo de la víctima, sino de todos sus contactos cuando se hace pasar por él.

Tampoco incluyen herramientas que comprueben la autenticidad de los archivos que se envían a través de ellos, aumentando así la posibilidad de esconder virus o troyanos. Por lo anterior, el acceso al Messenger no será posible para ningún funcionario.

4.5.4.6. Descargas (Transferir Programas)

Los programas gratuitos como protectores de pantalla y juegos que se descargan de sitios Web a menudo son fuentes de virus. Por lo tanto NO se deben descargar estos programas.

4.5.4.7 Correo Electrónico

Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros de la empresa y están sujetos a monitoreo y auditoria.

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional de la empresa.

El correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con las políticas internas.

Si se recibe un mensaje de correo electrónico con un archivo adjunto sospechoso, no se abrirá, incluso si conoce al emisor. No habrá archivos adjuntos de fuentes desconocidas o de emisores que no esté esperando; el encarado de la seguridad, desactivará la apertura automática de archivos adjuntos de correo electrónico.

A través del uso de correo electrónico se evitará lo siguiente:

- Provocar problemas legales a la empresa.
- Utilizar esta herramienta para fines lucrativos personales.
- Contravenir las políticas de la empresa.
- Atentar contra la imagen y buen nombre de la empresa.
- Interferir con el trabajo de los demás funcionarios y empleados.

Todo funcionario que tenga dudas acerca del material que puede enviar o recibir, debe consultarlo con su jefe inmediato.

Está prohibido lo siguiente:

- Leer, borrar, copiar o modificar correos electrónicos de otros usuarios.
- Enviar mensajes de acoso, obscenos o amenazadores a otro usuario.
- Envío de correo electrónico basura, mensajes con ánimo de lucro o mensajes en cadena.

- Interceptar el correo electrónico de otros usuarios.
- Enviar correo electrónico, utilizando el nombre del usuario y la contraseña de otro funcionario, sin su debida autorización.
- Enviar mensajes de manera masiva, por ejemplo, cadenas de cartas y relativos a falsos virus, excepto si contienen información de interés institucional.
- Mensajes de carácter religioso, superación personal, así como chistes y bromas.
- Cualquier otro uso indebido.

4.5.4.8. Seguridad de contraseñas

Es importante que todos los empleados protejan sus contraseñas, debiéndose seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se escribirán las contraseñas en papel, o se almacenarán en medios digitales no encriptados (con clave).
- Las contraseñas no serán divulgadas a ningún otro usuario. Si se divulga, esta será cambiada durante el próximo ingreso.
- El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.
- Los sistemas no mostrarán la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.

- Las contraseñas deben estar siempre encriptadas cuando se encuentren almacenadas o cuando sean transmitidas a través de redes.
- El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.
- No utilizar palabras simples, que pueden ser encontradas fácilmente.
- No comentar a nadie su clave de acceso.
- Las claves de acceso se deben memorizar y no anotar.

- La longitud de la clave de acceso debe ser de mínimo seis (6) caracteres de tipo alfanumérico y que combine al menos 2 características como mayúsculas, minúsculas, números.

Las claves de acceso son la barrera para evitar ingresos no autorizados a los sistemas de información de la empresa. Todos los empleados protegerán sus contraseñas y acatarán las siguientes regulaciones:

4.5.4.9. Control de acceso a redes

El Objetivo es Prevenir el acceso no autorizado a los servicios de red

Conexiones con redes externas: Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos (ADSL, dial-in) y conexiones con redes externas, exponen a los sistemas de la empresa a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten

con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto.

- Todos los enlaces de la red contarán con niveles de seguridad adecuados para proteger de ataques directos o indirectos a los activos más valiosos de las unidades de negocio, esto es la información, para minimizar que los sistemas de red sean vulnerables y presenten mayores niveles de riesgo por los accesos remotos y conexiones con redes externas.

- Todas las conexiones realizadas entre la red interna de la empresa e Internet serán controladas por un firewall para prevenir accesos no autorizados. El departamento de sistemas aprobará todas las conexiones con redes o dispositivos externos.
- El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que "hackers" u otras personas pueden obtener fácilmente información sobre la estructura de red de la empresa y computadoras internas.
- Para eliminar las vulnerabilidades inherentes al protocolo TCP/IP, ruteadores y firewalls deben rechazar conexiones externas que parecieran originarias de direcciones internas (ip spoofing- ip de suplantación de identidad)

Conexiones permitidas por el firewall: Conforme los requerimientos de las aplicaciones empleadas por la empresa y las políticas de acceso a servicios de red,

se deberá configurar en el firewall todos los puertos de acceso que serán habilitados y/o deshabilitados.

Estándares generales: Los accesos a los recursos de información deben solicitar como mínimo uno de los tres factores de autenticación:

- Factor de conocimiento: algo que solo el usuario conoce. Por ejemplo: contraseña
- Factor de posesión: algo que solo el usuario posee. Por ejemplo: nombre de usuario único
- Factor biométrico: algo propio de las características biológicas del usuario. Por ejemplo: lectores de huellas digitales.

Todos los componentes de la red deben mostrar el siguiente mensaje de alerta en el acceso inicial.

Todos los componentes de la red de datos deben ser identificados de manera única y su uso restringido. Esto incluye la protección física de todos los puntos vulnerables de una red. Las estaciones de trabajo y computadoras personales deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentren desatendidas.

Todos los dispositivos de red, así como el cableado deben ser ubicados de manera segura. Cualquier unidad de control, concentrador, multiplexor o procesador de

comunicación ubicado fuera de una área con seguridad física, debe estar protegido de un acceso no autorizado.

Política del uso de servicio de redes: Los usuarios solo deben tener acceso a los servicios que han sido específicamente autorizados a utilizar. Todas las conexiones de red internas y externas deben cumplir con las políticas de la empresa sobre servicios de red y control de acceso. Es responsabilidad del área de seguridad determinar lo siguiente:

- Elementos de la red que pueden ser accedidos
- El procedimiento de autorización para la obtención de acceso
- Controles para la protección de la red.

Todos los servicios habilitados en los sistemas deben contar con una justificación coherente con las necesidades del negocio. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio.

Segmentación de redes: La arquitectura de red de la empresa debe considerar la separación de redes que requieran distintos niveles de seguridad. Esta separación debe realizarse de acuerdo a la clase de información albergada en los sistemas que constituyen dichas redes. Esto debe incluir equipos de acceso público.

Encriptación de los datos: Las contraseñas, los códigos o números de identificación personal y los identificadores de terminales de acceso remoto deben

encontrarse encriptados durante la transmisión y en su medio de almacenamiento. La encripción de datos ofrece protección ante accesos no autorizados a la misma.

Aspecto eléctrico y de red

- Todos los equipos informáticos deben estar conectados a un UPS central
- No se deben tener extensiones ni cables sueltos cerca de los equipos.
- Todos los equipos deben tener protección contra cortocircuitos y sobre voltaje ya sea interna o externa.
- Se debe verificar diariamente el correcto funcionamiento de las lámparas y tomacorrientes ubicados en el centro de servidores y cableado.
- Se debe revisar periódicamente todos los mensajes y el menú de control de la UPS, para precisar el estado general de la misma, sus parámetros de medición, el estado de las baterías y alarmas y la configuración del sistema. Para luego confrontarlos con los valores requeridos y recomendados por el proveedor.
- Se debe asegurar una buena ventilación, asilamiento y aireación de la UPS.
- Se debe definir una política de finalización de tareas con el objetivo de disminuir gradualmente la carga del UPS, en el momento de una interrupción eléctrica, según las necesidades identificadas y a la potencia de las baterías.
- Se debe utilizar la toma que estén conectados a la UPS sólo para conectar los equipos de cómputo de misión crítica, en ningún momento pueden ser

conectados radios, grabadoras, lámparas, ventiladores, hornos microondas y otros.

- Todas las reparaciones de UPS debe ser realizada por personal especializado.
- Se debe proteger y colocar un mensaje en el botón **Emergency Power-Off** para evitar que sea presionado por personal no autorizado.
- El cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario y debe facilitar el mantenimiento y relocalización de áreas de trabajo.
- Para el cableado horizontal se debe emplear cable trenzado de cuatro pares UTP de nivel 6 para velocidades de hasta 100 Mbps
- No se deben realizar empates es decir múltiples apariciones del mismo par de cable en diversos puntos de la distribución.
- La distancia máxima del cable es de 90 metros independiente del cable utilizado, distancia entre el área de trabajo y el centro de cableado.
- El cable de empate del equipo y el punto de red llamado Path Cord debe ser máximo de 3 metros.
- Los conectores terminales deben ser RJ-45 bajo el código de colores de cableado T568B
- El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1,25 cm.
- El radio de la curvatura del cable no debe ser menor a cuatro veces el diámetro del cable, para el cable UTP categoría 5 el radio mínimo es de 2.5cm.

- En la ruta del cableado de los closets a los nodos debe evitar el paso por dispositivos eléctricos como equipos de soldaduras, aire acondicionado, ventiladores, intercomunicadores, luces fluorescentes y balastos debe pasar mínimo a una distancia de de 12 cm.
- El cableado debe pasar mínimo a 1,2 metros de los motores eléctricos grandes o transformadores.
- Debe estar distante de los cables de corriente alterna con 2KVA ó menos 13 cm., de cables de 2 KVA a 5 KVA debe estar distante 30 cm. y de cables de 5 KVA mínimo 91 cm.
- Se debe ubicar en el centro de cableado el diagrama de cableado de la red, éste debe indicar claramente el diagrama de distribución, el puerto asignado a cada toma de información, a cada servidores y en general a cada una de las conexiones e interconexiones.
- Si no es posible enviar las conexiones por tuberías se debe realizar un aislamiento de las mismas utilizando canaletas.
- Se debe contratar el servicio externo de mantenimiento trimestral o semestral tanto preventivo como correctivo de equipos informáticos, con una empresa calificada.
- Todos los equipos informáticos deberán mantener configurados el ahorro de energía y debe existir una política para escritorios y pantallas limpias.

4.5.4.10. Protección contra codigo mailicioso y movible (virus)

El Objetivo es Proteger la integridad del software y de la información.

Los virus pueden dañar o eliminar archivos, o incluso borrar todo el disco duro.

Si el software de protección contra virus no está actualizado, ofrece una protección muy débil contra nuevos virus; para mitigar este suceso, el departamento de sistemas debe instalar software antivirus fiable y examinar regularmente los sistemas para comprobar que no haya virus. Lo más importante es actualizar el software de forma frecuente.

- El área encargada de seguridad debe implementar controles de detección, prevención y recuperación para la protección contra código mailicioso, y procedimientos adecuados de toma de conciencia de los usuarios.

- Es obligación del personal encargado de seguridad de la empresa, emplear sólo los programas antivirus cuyas licencias han sido adquiridas por la empresa.
- El programa antivirus debe encontrarse habilitado en todos las computadoras de la empresa y será actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas se comunicarán al área de sistemas. El programa antivirus será configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la empresa. Debe contarse con un procedimiento para su actualización periódica.

- Se evitará compartir directorios o archivos con otros usuarios; en caso de ser absolutamente necesario, se coordinará con el Departamento de Sistemas.
- Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar el equipo de la red de datos, notificar al área de sistemas quien brindara soporte técnico, para la eliminación del virus antes de restablecer la conexión a la red de datos.
- Es responsabilidad del usuario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.
- Ante un indicio de contaminación por un virus informático nuevo o desconocido, se procederá a aislar y/o apagar el equipo y preservar la computadora infestada y comunicarse de inmediato con la empresa proveedora del antivirus.
- El responsable de la seguridad informática debe llevar un registro de los virus que aparezcan en la entidad y tratar de determinar quienes lo introducen y como, sea de forma intencional o no.
- El programa antivirus debe estar configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la empresa.
- La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. Se tomarán medidas disciplinarias en caso se encuentren dichos programas en computadoras personales de usuarios.

Está prohibido el uso de diskettes, flash memory´s y discos compactos provenientes de otra fuente que no sea la de la misma empresa. La excepción se da cuando estos dispositivos provienen de las interfaces con organismos reguladores, proveedores y clientes, los cuales obligatoriamente deben pasar por un proceso de verificación y control en el departamento de Sistemas, antes de ser leídos.

4.5.5 Administración de la red.

Para tener una completa seguridad de que todas las partes de la red aun las más pequeñas, sean funcionales, es imperativo evaluar los componentes de la red. Realizar esta operación habilita para perfeccionar las sugerencias de sus usuarios al hacerlas más eficaces y útiles para responder a las necesidades de los mismos.

En nuestro caso, la administración de la red, implica mantenerla en perfecto funcionamiento, para ello se necesita tener los informes respectivos de algunos tipos de evaluaciones, referidas esencialmente al funcionamiento de la misma, entre las muchas evaluaciones posibles, las más recomendadas son:

- Tiempo de intervenciones de mantenimiento.
- Tiempo de reparación de una falla.
- Tiempo de instalación de un nuevo cable.
- Tiempo de intervención en el caso de una solicitud de apoyo.
- Horas de utilización de la red, por usuario, estación, etc.
- Cantidad de estaciones instaladas y verificadas.

- Cantidad de aplicaciones instaladas.
- Número de intervenciones de reparación.
- Índice de errores.
- Otros índices de satisfacción del usuario.

La administración de una red estará a cargo del departamento de tecnologías o del técnico informático que labore en la empresa. La importancia del proceso administrativo de una red se puede ilustrar en el siguiente esquema.

4.6 VALIDACIÓN DE LA PROPUESTA.

Luego de disponer de la red, primeramente se procedió a activar el software comercial que dispone la empresa y que sirve especialmente para el control de ventas e inventarios. Esto software es multiusuario y permite actualmente consultar las existencia en la matriz y sucursal. A más dE ello el proceso de facturación continúa en forma normal.

Consultando a los involucrados en la problemática podemos apreciar que al disponer de un conocimiento real de la existencia en la bodega se han podido canalizar mucho mejor las ventas, complementariamente a esto el sistema de facturación hace que toda la gestión de ventas se vea mejorada para el beneficio empresarial.

4.7 CONCLUSIONES

- Como resultado del análisis de la red se encontró que el sistema de comunicaciones es precario, y no cubre las necesidades o requerimientos de los usuarios, ya que no tiene una adecuada estructuración. Por esta razón hacen uso de otros medios de comunicación como mensajería tradicional y correos electrónicos.
- Los problemas en la comunicación generan pérdidas de recursos tiempo, dinero, y además la falta de seguridad en la transmisión de un activo tan importante para la organización como lo es la información.
- La red diseñada se constituye en un elemento importante dentro de la gestión comercial de la empresa. Este se debe a que se pueden optimizar las ventas, así como las consultas sobre el inventario existente
- La red permite que se tomen decisiones acertadas y a tiempo en cuanto al aspecto comercial de la empresa, esto también implica la incorporación de nuevos servicios como pagos con tarjeta de crédito, etc.
- Las redes Inalámbricas se han popularizado hoy en día debido a su bajo costo, esto ha permitido que con una baja inversión se logre mejorar el aspecto comercial de la empresa
- A futuro se pueden incorporar nuevas tecnologías a ser usadas en la red, así por ejemplo se puede incorporar el servicio telefónico de voz sobre IP al interior de la empresa, también se puede disponer de un sistema de monitoreo remoto con video. Estas actividades implicaran un ahorro en la economía de la empresa y son parte del beneficio que produce la red.

4.8 RECOMENDACIONES

- Implementar algunos de los programas para elevar la seguridad y eficiencia de la red. También puede adquirirse firewall físicos de seguridad
- Capacitar al personal sobre el manejo de redes.
- Renovar el parque informático de la empresa, así como ampliarlo

BIBLIOGRAFÍA

ÁVILA Pesantez Diego; Redes de Computadores; Editorial Universitaria; 2001

IZIQUE Julio C; Redes Inalámbricas; 2004

ROBBINS Stephen P & Decenzo David A; Fundamentos de Administración; Editorial Universitarios; Tercera Edición; 2002

- Artículo publicado en la Revista GIGATRONIC 14, nov del 2001

www.monografias.com/trabajos14/redes/redes.shtml

Temas: - Redes

- Topologías de redes

www.abcdatos.com/tutoriales/tutorial/127.html

Tema: - Redes Ethernet

http://es.wikipedia.org/wiki/switch

Temas: - Conmutadores (switch)

- Características de los switch

- Como trabajan los switch

http://www.teletronics.com/WLAccespoint.html

Tema: - Access Point