MEJORAMIENTO LAN BIOCHEM FARMACÉUTICA

MIGUEL ALBERTO MARTNEZ
JORGE OCTAVIO GALEANO PARDO
JOHAN ELVIS LASSO GALEANO

CORPORACIÒN UNIVERSITARIA UNITEC
FACULTAD DE TECNOLOGIA EN SISTEMAS Y ELECTRONICA
DIPLOMADO EN ADMINISTRACION Y SEGURIDAD DE REDES
BOGOTA D.C.
2006

MEJORAMIENTO LAN BIOCHEM FARMACÉUTICA

MIGUEL ALBERTO MARTNEZ
JORGE OCTAVIO GALEANO PARDO
JOHAN ELVIS LASSO GALEANO
36012044
46012013
36021122

Asesor de Investigación:
Manuel Oliver Domínguez.

CORPORACIÒN UNIVERSITARIA UNITEC
FACULTAD DE TECNOLOGIA EN SISTEMAS Y ELECTRONICA
DIPLOMADO EN ADMINISTRACION Y SEGURIDAD DE REDES
BOGOTA D.C.
2006

MEJORAMIENTO LAN BIOCHEM FARMACÈUTICA

Por

MIGUEL ALBERTO MARTNEZ
JORGE OCTAVIO GALEANO PARDO
JOHAN ELVIS LASSO GALEANO

CORPORACIÒN UNIVERSITARIA UNITEC

2006

Aprobada por:

_____

Firma del presidente del jurado

_____

_____

_____

Programa autorizado para obtener el díplomado

_____

Ciudad y Fecha

_____

AGRADECIMIENTOS

Agradecemos los aportes que se tuvieron de los docentes de la Facultad de Tecnología de Electrónica y Telecomunicaciones y Sistemas de la Coorporación Universitaria UNITEC por sus invaluables conocimientos.

TABLA DE CONTENIDO

INTRODUCCION 3

OBJETIVOS 4

ALCANCE 5

DEFINICIÓN DEL PROBLEMA 6

1. MARCO TEORICO 7
1.1 TIPOS DE REDES 8
1.1.1 Redes En Estrella 8
1.1.2 Redes En Anillo 8
1.1.3 Redes En Forma De Bus 9
1.2 TIPOS DE CABLE 9
1.2.1 Especificaciones De Cables 9
1.2.2 Cable Coaxial 11
1.2.3 Cable STP 12
1.3 FIBRA ÓPTICA 15
1.3.1 Reflexión 15
1.3.2 Concepto De Fibra Óptica 16
1.3.3 Caracteristicas 16
1.3.4 Ventajas 16
1.3.5 Desventajas 17
1.3.6 Fibra Multimodo 17
1.3.7 Fibra Monomodo 21
1.3.8 Otros Componentes Ópticos 22
1.3.9 Instalación, Cuidado Y Prueba De La Fibra Óptica 25
1.4 DISPOSITIVOS DE LAS DIFERENTES CAPAS 27
1.5 CAPA FÍSICA DE LA LAN 27
1.5.1 Cables De Fibras Ópticas Para Redes Lan 28
1.6 SERVIDOR DE DHCP 28
1.6.1 Caracteristicas 29
1.6.2 Ventajas Del Uso De DHCP 29
1.6.3 Asignación De Direcciones IP 30
1.6.4 Motivos Para Usar El Protocolo DHCP 30
1.6.5 Funcionamiento Del Servidor DHCP 31
1.6.6 Parámetros Configurables 31
1.6.7 El Servidor DNS 32
1.6.7.1 Historia Del DNS 32
1.6.8 Puerta De Enlace 33
1.6.9 Máscara De Red 33
1.6.10 Protocolo ARP 34
1.6.10.1 Tablas ARP 35
1.6.11 Protocolo FTP 35
1.6.11.1 Introducción a File Transfer Protocol (FTP): 36
1.6.11.2 Algunas Definiciones FTP 36
1.6.12 PROXY 37
1.6.12.1 Ventajas 37

1.6.13 FIREWALL 37
1.6.13.1 Ventajas De Un FIREWALL 38
1.7 VLANs 39
1.7.1 Clases De VLAN 42
1.7.2 Generaciones De VLAN 43
1.7.3 VLAN Por Puerto 43
1.7.4 VLAN por MAC 44
1.7.5 VLAN por Protocolo 44
1.7.6 VLAN Por Subredes De IP o IPX 44
1.7.7 VLAN Definidas Por El Usuario 44
1.7.8 VLAN Binding 44
1.7.9 VLAN por DHCP 44
1.8 PACKET SNIFFER 45
1.8.1 Topología de red y packet sniffers 45
1.8.2 Utilidad 46
2. ESTUDIO ACTUAL DE LA RED 47
2.1 DESCRIPCIÓN Y DISPOSITIVOS DE LA RED 47
2.1.1 Dispositivos De Red: 47
2.1.2 Dispositivos Hardware: 47
3. DIAGNOSTICO DE LA RED 53
3.1 PRIMER PROBLEMA 53
3.2 SEGUNDO PROBLEMA 60
3.2.1 ZoneAlarm 61
3.2.2 CProxy Anonymity 4 Server 3.4. 64
3.3 TERCER PROBLEMA 64
3.3.1 Switch Cisco Catalyst Express 500-24TT 65
3.3.2 ROUTER Cisco 1811 66
3.3.3 Grafica Con respecto al tráfico 67
4. COSTO DEL PROYECTO 70

RECOMENDACIONES 71

CONCLUSIONES 72

BIBLIOGRAFÍA 73

INTRODUCCION

Debido a la modernización de las comunicaciones y a las necesidades que crecen cada dia al paso del tiempo en las empresas, organizaciones o compañías, la idea o el objetivo de mejorar cada vez la calidad laboral y humana, con el fin de desarrollar soluciones e implementando nuevas tecnologías hacen que las redes de datos sean indispensables para el buen funcionamiento de las comunicaciones de las compañias.

Actualmente el tráfico entre redes, subredes de la red en si misma se han incrementado debido a que empresas no ven la posibilidad de actualizar nuevas tecnologias.

Uno de los motivos por el cual el desarrollo laboral se decrementa es porque los empleados no están desempeñando totalmente sus labores para la que fueron contratados, normalmente utilizan servicios no indispensables para la compañía, servicios como por ejemplo: Chat, Messenger, multimedia, etc. Se hace indispensable la cancelación de estos servicios por medio de herramientas instaladas en un servidor como un Proxy y Firewall.

OBJETIVOS

Objetivo General

- Sustituir el enlace UTP por una conexión más estable, menos ruidosa para la interconexión de las dos sedes de Biochem Farmacéutica.

Objetivos Específicos

- Implementar un servidor Windows Server para el control de seguridad y acceso a diferentes servicios implicando el control laboral de las diferentes estaciones de trabajo.

- Implementar el desarrollo de Redes VLANS en los departamentos de Biochem Farmacéutica.

ALCANCE

Se va ha implementar la solución de una red en donde su alcance llega hasta la sede norte de Biochem farmacéutica ubicada en la Carrera 41 # 167 –30, donde se cumpla con los objetivos anteriormente señalados y que sea capaz de solucionar los problemas actuales de la empresa.

DEFINICIÓN DEL PROBLEMA

La red de Biochem Farmacéutica actualmente esta compuesta por dos Edificios ubicados en la Carrera 41 # 167 –30, la primer sede posee 30 estaciones de trabajo, la segundad sede posee 13 con sus respectivos departamentos y estas están interconectadas por un enlace UTP de 50 metros *Categoría 5E*.

Esto no quiere decir que existe mas de dos subredes, en realidad la red es un conjunto de una sola red, esto implica que con el paso del tiempo y si se quiere expandir la red se tendrá un incremento de trafico debido a que no hay segmentación.

El otro problema a cuestionar es el enlace de interconexión de las dos sedes ya que puede presentar un problema entre los distintos departamentos por lo que se decrementa el rendimiento de la red y el nivel laboral de la empresa. Este tipo de problemática se debe a factores climáticos y tecnológicos que afectan la comunicación.

A pesar de que no es prioridad y actualmente la labores actuales son realizadas con los conflictos que existen, otro de los retos actuales en la empresa es el problema de la administración y control de servicios adicionales e innecesarios para las funciones laborales como por ejemplo:

- Messenger
- Descarga de archivos multimedia
- Descarga de ficheros peligrosos

Debido a esta preocupación por la que se afecta el rendimiento laboral las empresas y grandes compañías siempre buscan la implementación de sistemas de control a estos servicios, por lo tanto es necesario aplicar nuevos tipos de tecnología para el mejor uso de la jornada laboral.

1. MARCO TEORICO

La denominación «**Local Área Networks**» (LAN) - redes locales - fue introducida con el fin de establecer la delimitación, por una parte, con respecto al acoplamiento de procesadores con muy altas velocidades de transmisión y longitudes extremadamente cortas y, por otra, con respecto a redes de tráfico para grandes distancias con tasas de información relativamente bajas pero grandes extensiones. Las distancias entre las diversas estaciones de una red LAN varian, habitualmente, entre 100 m y algunos kilómetros; las velocidades de transmisión oscilan entre 100 Kbit/s y en algunos casos 100 Mbit/s.

Se puede definir que una red local es una red para la transmisión de información con secuencia en serie de bits entre equipos independientes, entre sí e interconectados. Es de competencia total del usuario y está limitada a su predio.

De acuerdo a la topología, los criterios de uso, las intersecciones y métodos de acceso así como sus medios de transmisión. La distribución de la información se realiza por lo general con paquetes de datos en canales sin asignación fija, contrariamente a la mayoría de los usos en la técnica analógica y digital, donde por ejemplo al llamar por teléfono un canal de transmisión determinado es asignado al abonado durante el tiempo que permanece comunicado.

Los usos de la redes LAN se dan ante todo en el ámbito de la ofimática (correo electrónico etc.), del enlace de computadores personales así como en el ámbito industrial (control de procesos, etc.).

Para las redes LAN se requieren por lo general redes de cables coaxiales o de conductores de fibras ópticas separadas de la red telefónica. La transmisión se efectúa con velocidades que varían entre 0,1 Mbit/s y aproximadamente 100 Mbit/s.

El principal criterio para la elección, desde el punto de vista técnico de los medios de transmisión, es el de la rentabilidad del sistema respectivo. Los sistemas que actualmente se ofrecen en el mercado (con velocidades de transmisión de 0,1 hasta aprox. 20 Mbit/s) en su mayor parte aún se operan con cables de cobre, simétricos y coaxiales.

Sin embargo, se percibe claramente el avance de los sistemas basados en conductores de fibras ópticas, ya que este presenta muchas ventajas, como baja atenuación, gran ancho de banda, separación galvánica de los abonados, alta seguridad contra escuchas e insensibilidad contra perturbaciones eléctricas, todo

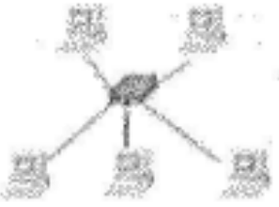
lo cual permite llegar, con respecto a cables coaxiales, a alcances considerablemente más extensos sin regenerador intermedio. Según la valoración de las características señaladas resultan usos que sólo son posibles.

1.1 TIPOS DE REDES

1.1.1 Redes En Estrella

Para las configuraciones de redes en estrella, además de cables coaxiales son apropiados los cables de fibra óptica. Su especificación básica esta confeccionada según Ethernet. Sus valores tipicos son 1 Mbit/s con el método de acceso de CSMA/CD (**Carrier Sense Multiple Access with Collision Detection**, también especificado en IEEE 802.3). (Capítulo 11.3.3). En los puntos nodales de estas redes existen acopladores en estrella activos, desde los cuales los cables de fibras ópticas se dirigen al correspondiente equipo terminal, al siguiente acoplador en estrella. Se habla de redes LAN ópticas activas con una extensión de hasta 5 Km. y velocidades de transmisión de hasta 10 Mbit/s.

Configuración en estrella



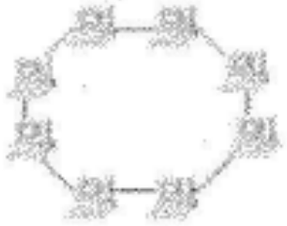
1.1.2 Redes En Anillo

En el caso de las redes en anillo se pueden aplicar en muchas formas cables con fibras ópticas. Las señales son transmitidas de estación a estación, hasta haber alcanzado la estación receptora o recibir en retorno su propio paquete de datos. Con cada retransmisión se regenera la señal. Para adjudicar la habilitación de transmisión se ha impuesto, principalmente, el método denominado «**Token Access**» (especificada en IEEEZ) 802.5). Un «**Token**» (signo de identificación, comprobante) va pasando en el anillo de estación en estación; la posesión del **token** habilita para transmitir un paquete de información.

Las velocidades de transmisión y extensiones de redes como las señaladas superan a aquellas de los sistemas de bus con banda básica, es decir que pueden

alcanzar valores de hasta 100 Mbit/s y extensiones de 4 hasta 10 km. Sin embargo, los tiempos de espera son más largos, en función de los paquetes de datos.

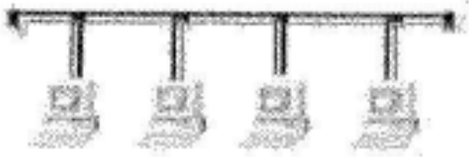
Configuración en anillo



1.1.3 Redes En Forma De Bus

Los sistemas de banda básica especificados según Ethernet ya han logrado imponerse para numerosos usos. Para los sistemas en forma de bus, se utiliza como medio de transmisión cables especiales de cobre, simétricos y coaxiales así como - para extender los trayectos - cables de fibras ópticas. Los datos son transmitidos por medio de un acoplamiento pasivo por el cable coaxial hacia ambos lados, y destruidos en los extremos mediante resistencias terminales libres de reflexiones.

Configuración en Bus



1.2 TIPOS DE CABLE

1.2.1 Especificaciones De Cables

Los cables tienen distintas especificaciones y generan distintas expectativas acerca de su rendimiento.

- ¿Qué velocidad de transmisión de datos se puede lograr con un tipo particular de cable? La velocidad de transmisión de bits por el cable es de suma importancia. El tipo de conducto utilizado afecta la velocidad de la transmisión.
- ¿Qué tipo de transmisión se planea? ¿Serán las transmisiones digitales o tendrán base analógica? La transmisión digital o de banda base y la transmisión con base analógica o de banda ancha son las dos opciones.

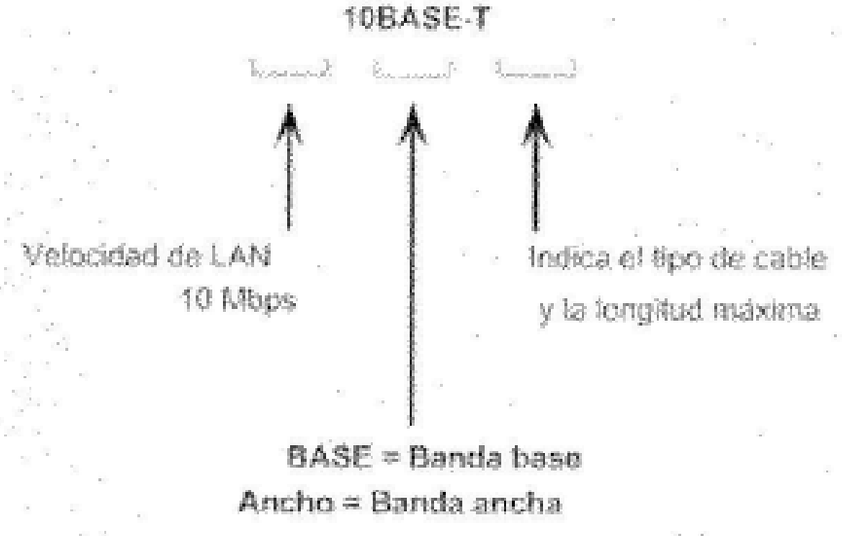
- ¿Qué distancia puede recorrer una señal a través de un tipo de cable en particular antes de que la atenuación de dicha señal se convierta en un problema? En otras palabras, ¿se degrada tanto la señal que el dispositivo receptor no puede recibir e interpretar la señal correctamente en el momento en que la señal llega a dicho dispositivo? La distancia recorrida por la señal a través del cable afecta directamente la atenuación de la señal. La degradación de la señal está directamente relacionada con la distancia que recorre la señal y el tipo de cable que se utiliza.

Algunos ejemplos de las especificaciones de Ethernet que están relacionadas con el tipo de cable son:

- 10BASE-T
- 10BASE5
- 10BASE2

10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.

10BASE5 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 5 representa la capacidad que tiene el cable para permitir que la señal recorra aproximadamente 500 metros antes de que la atenuación interfiera con la capacidad del receptor de interpretar correctamente la señal recibida. 10BASE5 a menudo se denomina "Thicknet". Thicknet es, en realidad, un tipo de red, mientras que 10BASE5 es el cableado que se utiliza en dicha red.



10BASE2 se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. El 2, en 10BASE2, se

refiere a la longitud máxima aproximada del segmento de 200 metros antes que la atenuación perjudique la habilidad del receptor para interpretar apropiadamente la señal que se recibe. La longitud máxima del segmento es en realidad 185 metros. 10BASE2 a menudo se denomina "Thinnet". Thinnet es, en realidad, un tipo de red, mientras que 10BASE2 es el cableado que se utiliza en dicha red.

1.2.2 Cable Coaxial

El cable coaxial consiste de un conductor de cobre rodeado de una capa de aislante flexible. El conductor central también puede ser hecho de un cable de aluminio cubierto de estaño que permite que el cable sea fabricado de forma económica. Sobre este material aislante existe una malla de cobre tejida u hoja metálica que actúa como el segundo hilo del circuito y como un blindaje para el conductor interno. Esta segunda capa, o blindaje, también reduce la cantidad de interferencia electromagnética externa. Cubriendo la pantalla está la chaqueta del cable.

Para las LAN, el cable coaxial ofrece varias ventajas. Puede tenderse a mayores distancias que el cable de par trenzado blindado STP, y que el cable de par trenzado no blindado, UTP, sin necesidad de repetidores. Los repetidores regeneran las señales de la red de modo que puedan abarcar mayores distancias.

El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos, incluida la televisión por cable.

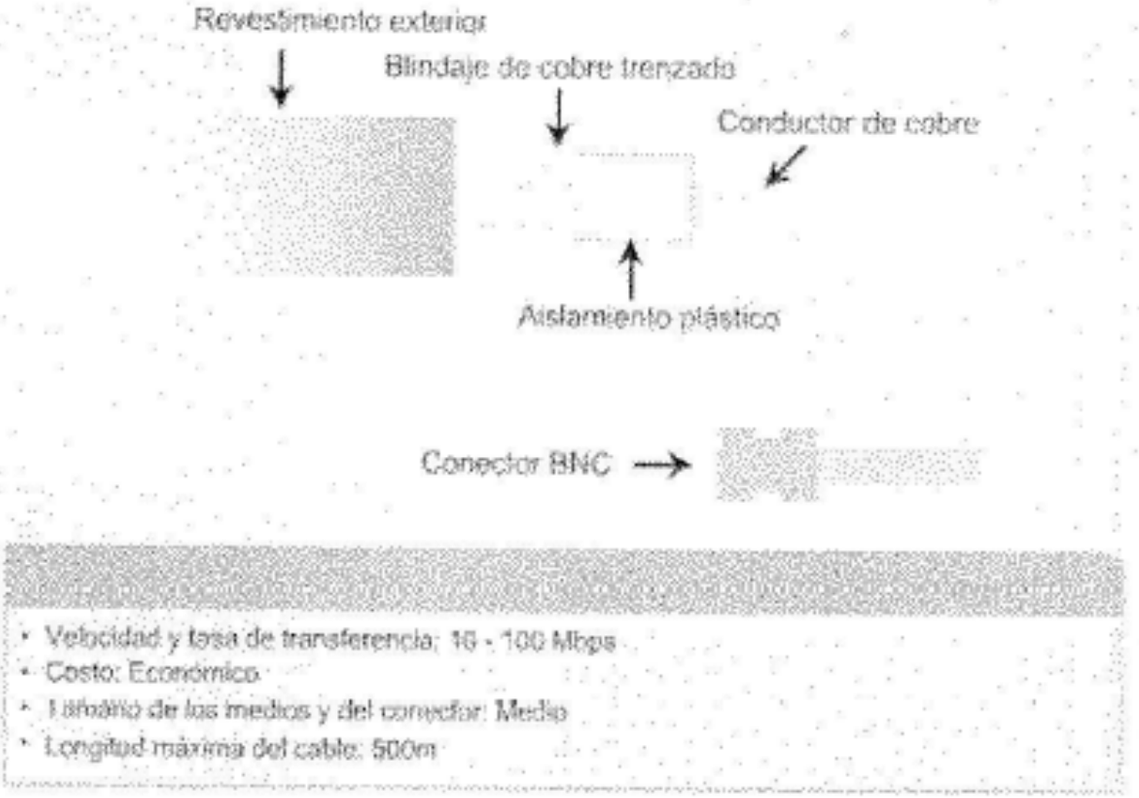
Al trabajar con cables, es importante tener en cuenta su tamaño. A medida que aumenta el grosor, o diámetro, del cable, resulta más difícil trabajar con él. Recuerde que el cable debe pasar por conductos y cajas existentes cuyo tamaño es limitado.

Se puede conseguir cable coaxial de varios tamaños. El cable de mayor diámetro es de uso específico como cable de backbone de Ethernet porque tiene mejores características de longitud de transmisión y de limitación del ruido. Este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa. Como su apodo lo indica, este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. Generalmente, cuanto más difícil es instalar los medios de red, más costosa resulta la instalación. El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet casi nunca se usa, salvo en instalaciones especiales.

En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm. (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para las instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación de thinnet era más sencilla, también resultaba más económica.

Por este motivo algunas personas lo llamaban cheapernet (red barata). El trenzado externo metálico o de cobre del cable coaxial abarca la mitad del circuito eléctrico. Se debe tener especial cuidado de asegurar una sólida conexión eléctrica en ambos extremos, brindando así una correcta conexión a tierra. La incorrecta conexión del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial.

Los problemas de conexión resultan en un ruido eléctrico que interfiere con la transmisión de señales sobre los medios de networking. Por esta razón, thinnet ya no se usa con frecuencia ni está respaldado por los estándares más recientes (100 Mbps y superiores) para redes Ethernet.



1.2.3 Cable STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Según se especifica para el

uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como, por ejemplo, el acoplamiento de par a par y la diafonía.

El STP también reduce el ruido electrónico desde el exterior del cable, como, por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.

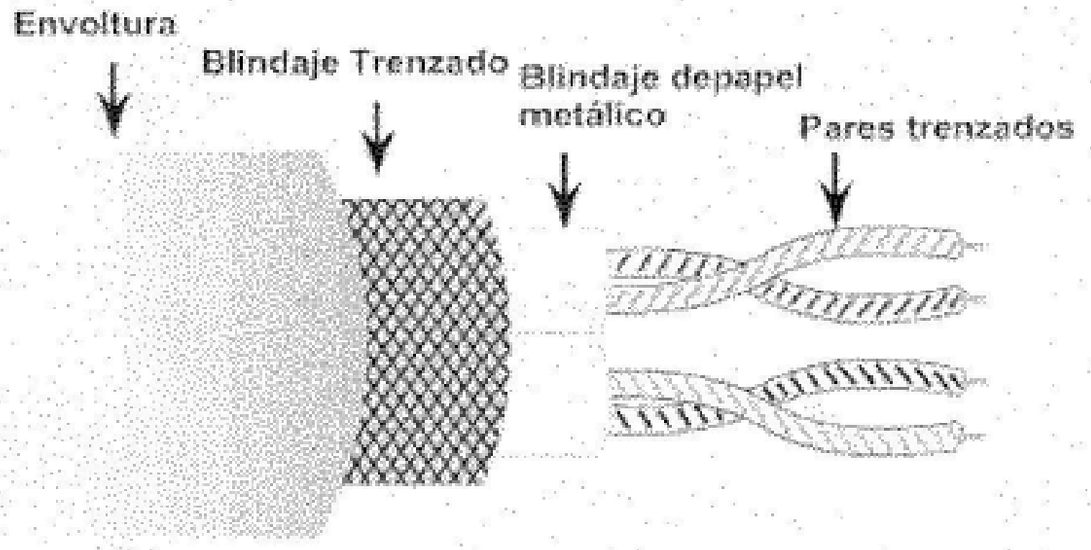
Un nuevo híbrido de UTP con STP tradicional se denomina UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El ScTP consiste, básicamente, en cable UTP envuelto en un blindaje de papel metálico. ScTP, como UTP, es también un cable de 100 Ohms. Muchos fabricantes e instaladores de cables pueden usar el término STP para describir el cable ScTP. Es importante entender que la mayoría de las referencias hechas a STP hoy en día se refieren en realidad a un cable de cuatro pares apantallado. Es muy improbable que un verdadero cable STP sea usado durante un trabajo de instalación de cable.

Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están adecuadamente conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el STP y el ScTP se pueden volver susceptibles a graves problemas de ruido.

Son susceptibles porque permiten que el blindaje actúe como una antena que recoge las señales no deseadas. Sin embargo, este efecto funciona en ambos sentidos. El blindaje no sólo evita que ondas electromagnéticas externas produzcan ruido en los cables de datos sino que también minimiza la irradiación de las ondas electromagnéticas internas. Estas ondas podrían producir ruido en otros dispositivos. Los cables STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios de networking (tales como el cable coaxial y la fibra óptica) sin que se repita la señal.

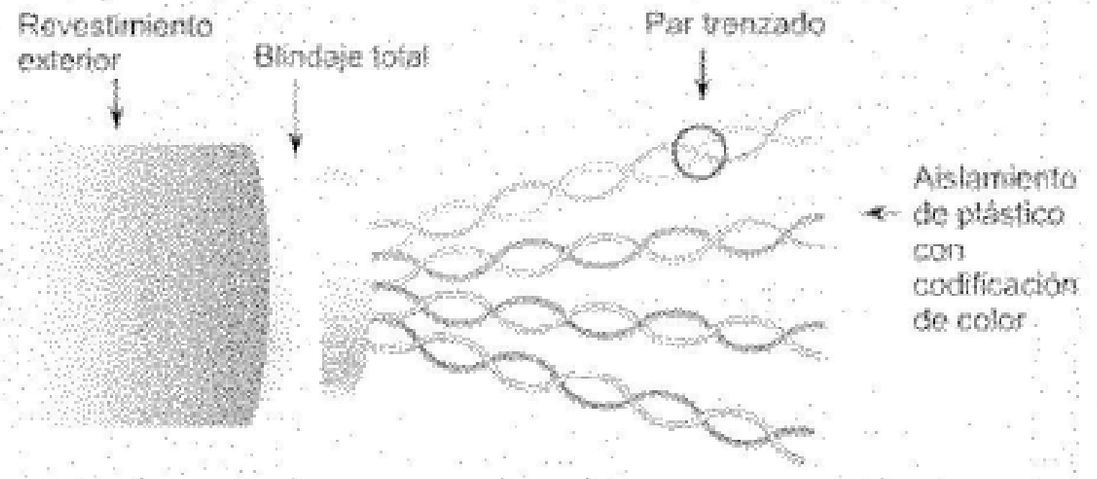
El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable. Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra. Sin embargo, el STP y el ScTP todavía desempeñan un papel importante, especialmente en Europa o en instalaciones donde exista mucha EMI y RFI cerca de los cables.

Cable de par trenzado blindado

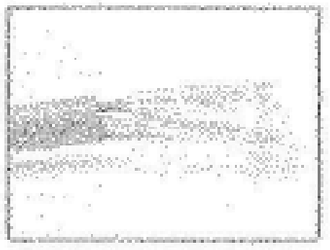


Velocidad y tasa de transferencia: 0 - 100 Mbps
Costo: Moderado
Tamaño de los medios y del conector: Mediano a grande
Longitud máxima del cable: 100m

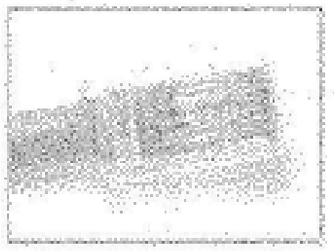
ScTP (Par trenzado apantallado)



Velocidad y tasa de transferencia: 0 - 100 Mbps
Precio promedio por nodo: Moderadamente caro
Tamaño de los medios y del conector: Mediano a grande
Longitud máxima del cable: 100m



Conector defectuoso: Los hilos están sin trenzar en un trecho demasiado largo.



Conector correcto: Los hilos están sin trenzar sólo en el trecho necesario para unir el conector.

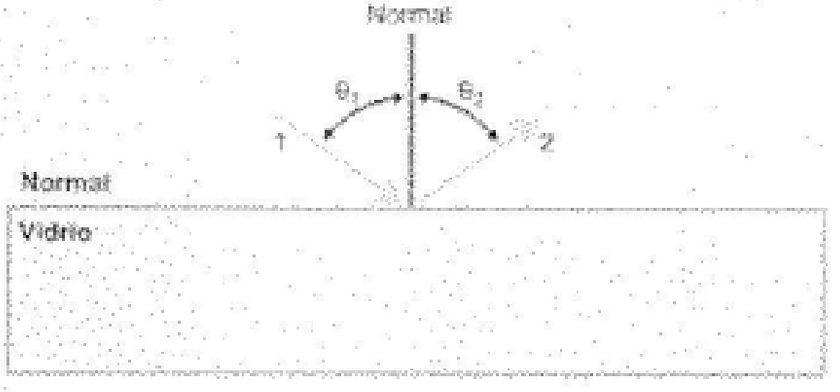
1.3 FIBRA ÓPTICA

1.3.1 Reflexión

Cuando un rayo de luz (el rayo incidente) llega a la superficie brillante de una pieza plana de vidrio, se refleja parte de la energía de la luz del rayo. El ángulo que se forma entre el rayo incidente y una línea perpendicular a la superficie del vidrio, en el punto donde el rayo incidente toca la superficie del vidrio, recibe el nombre de ángulo de incidencia.

Esta línea perpendicular recibe el nombre de normal. No es un rayo de luz sino una herramienta que permite la medición de los ángulos. El ángulo que se forma entre el rayo reflejado y la normal recibe el nombre de ángulo de reflexión.

La Ley de la Reflexión establece que el ángulo de reflexión de un rayo de luz es equivalente al ángulo de incidencia. En otras palabras, el ángulo en el que el rayo de luz toca una superficie reflectora determina el ángulo en el que se reflejará el rayo en la superficie.



Rayo 1: Rayo incidente, medido a θ_1 grados de la normal
Rayo 2: Rayo reflejado, medido a θ_2 grados de la normal
Ley de la reflexión: $\theta_1 = \theta_2$

La luz que viaja a través del aire se refleja en la superficie del vidrio.

1.3.2 Concepto De Fibra Óptica

Guía o conducto de ondas en forma de filamento, generalmente de vidrio (**polisilicio**), aunque también puede ser de materiales plásticos, capaz de transportar una potencia óptica en forma de luz, normalmente emitida por un láser o LED. Las fibras utilizadas en telecomunicación a largas distancias son siempre de vidrio, utilizándose las de plástico solo en algunas redes locales y otras aplicaciones de corta distancia, debido a que presentan mayor atenuación o posibilidad de sufrir interferencias.

1.3.3 Características

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

La fibra óptica ha representado una revolución en el mundo de las telecomunicaciones, por cuanto ha desplazado a los cables de cobre para la transmisión de grandes cantidades de información, sea en forma de canales telefónicos, televisión, datos, etc.

Como características de la fibra podemos destacar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad ya que son inmunes a las interferencias electromagnéticas de radio-frecuencia. Las fibras ópticas no conducen señales eléctricas, conducen rayos luminosos, por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión.

1.3.4 Ventajas

La fibra óptica se emplea en multitud de sistemas y el actual auge de los sistemas de banda ancha se debe en gran medida a la elevada capacidad de tráfico que pueden transmitir las redes de las operadoras basadas en fibra óptica. Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en los pequeños ambientes, y otra gran ventaja es dada la dificultad de hacer imperceptible una intercepción de los datos transmitidos.

- Gran flexibilidad y tenacidad.
- Diámetro, peso y radio de curvatura reducidos.
- Conectividad directa.

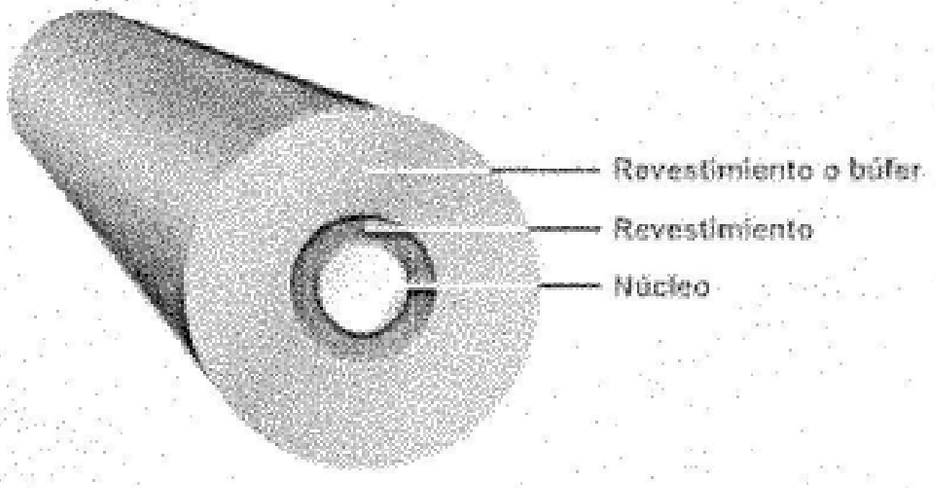
- No propagación de la llama.
- Resistencia a la humedad y a los roedores.
- Es inmune al ruido y las interferencias.
- Carencia de señales eléctricas en la fibra.
- El peso del cable de fibras ópticas es muy inferior al de los cables metálicos.
- La materia prima para fabricarla es abundante en la naturaleza.
- Compatibilidad con la tecnología digital.

1.3.5 Desventajas

- Fragilidad de las fibras.
- Dificultad de reparar un cable de fibras roto en el campo.
- Es un poco costoso.

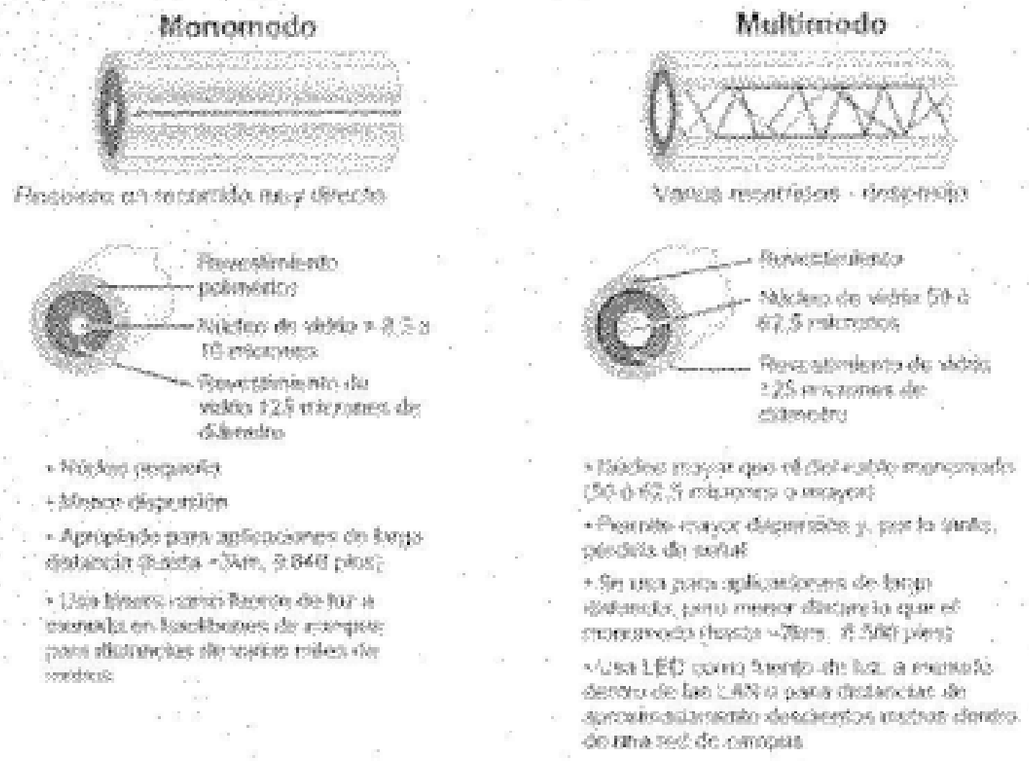
1.3.6 Fibra Multimodo

La parte de una fibra óptica por la que viajan los rayos de luz recibe el nombre de núcleo de la fibra.



Los rayos de luz sólo pueden ingresar al núcleo si el ángulo está comprendido en la apertura numérica de la fibra. Asimismo, una vez que los rayos han ingresado al núcleo de la fibra, hay un número limitado de recorridos ópticos que puede seguir un rayo de luz a través de la fibra.

Estos recorridos ópticos reciben el nombre de modos. Si el diámetro del núcleo de la fibra es lo suficientemente grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, esta fibra recibe el nombre de fibra "multimodo". La fibra monomodo tiene un núcleo mucho más pequeño que permite que los rayos de luz viajen a través de la fibra por un solo modo.



Cada cable de fibra óptica que se usa en networking está compuesto de dos fibras de vidrio envueltas en revestimientos separados. Una fibra transporta los datos transmitidos desde un dispositivo A a un dispositivo B. La otra transporta los datos desde el dispositivo B hacia el dispositivo A.

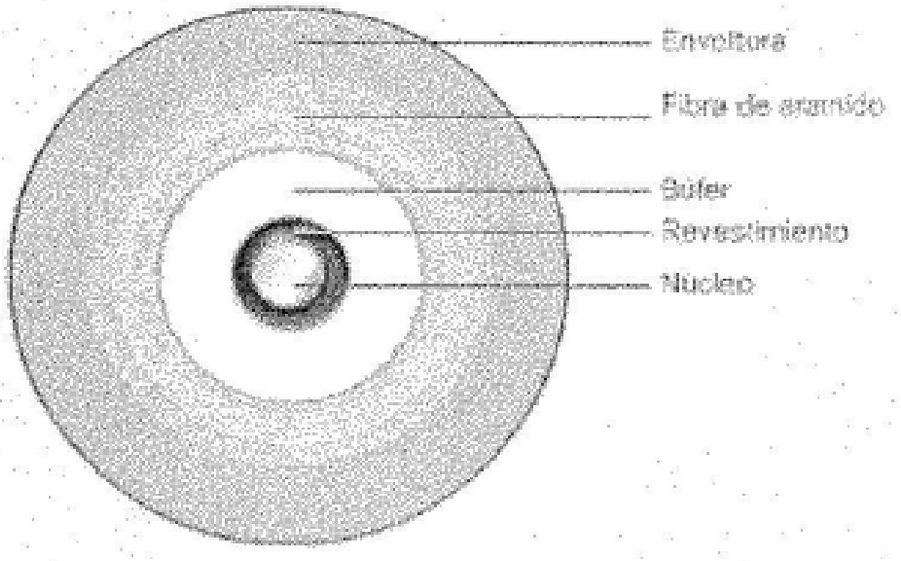
Las fibras son similares a dos calles de un solo sentido que corren en sentido opuesto. Esto proporciona una comunicación full-duplex. El par trenzado de cobre utiliza un par de hilos para transmitir y un par de hilos para recibir. Los circuitos de fibra óptica usan una hebra de fibra para transmitir y una para recibir. En general, estos dos cables de fibra se encuentran en un solo revestimiento exterior hasta que llegan al punto en el que se colocan los conectores.

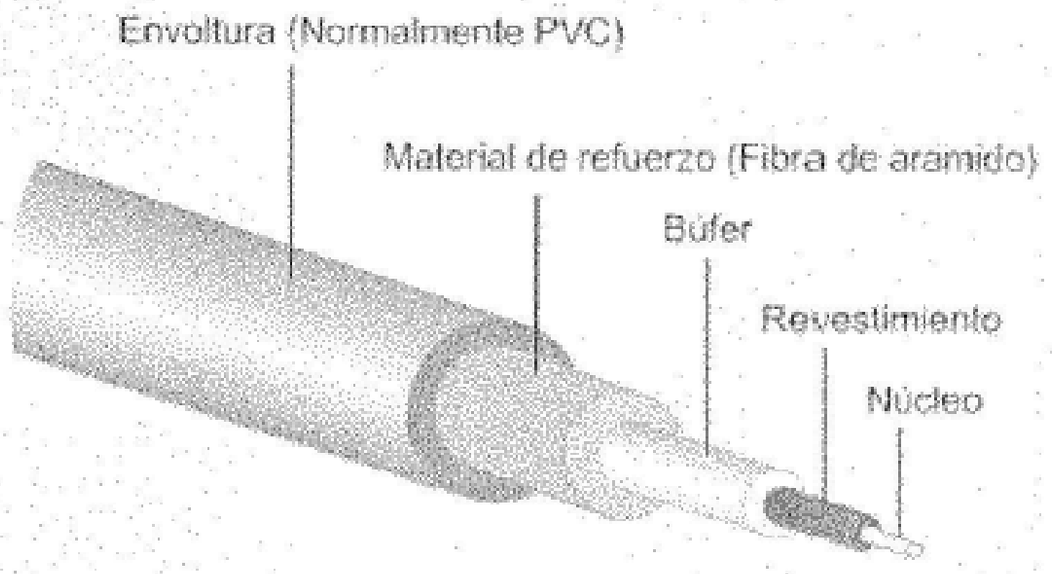
Hasta que se colocan los conectores, no es necesario blindar ya que la luz no se escapa del interior de una fibra. Esto significa que no hay problemas de diafonía con la fibra óptica.

Es común ver varios pares de fibras envueltos en un mismo cable. Esto permite que un solo cable se extienda entre armarios de datos, pisos o edificios. Un solo cable puede contener de 2 a 48 o más fibras separadas.

En el caso del cobre, sería necesario tender un cable UTP para cada circuito. La fibra puede transportar muchos más bits por segundo y llevarlos a distancias mayores que el cobre.

En general, un cable de fibra óptica se compone de cinco partes. Estas partes son: el núcleo, el revestimiento, un amortiguador, un material resistente y un revestimiento exterior.





El núcleo es el elemento que transmite la luz y se encuentra en el centro de la fibra óptica. Todas las señales luminosas viajan a través del núcleo. El núcleo es, en general, vidrio fabricado de una combinación de dióxido de silicio (sílice) y otros elementos. La fibra multimodo usa un tipo de vidrio denominado vidrio de índice graduado para su núcleo.

Este vidrio tiene un índice de refracción menor hacia el borde externo del núcleo. De esta manera, el área externa del núcleo es ópticamente menos densa que el centro y la luz puede viajar más rápidamente en la parte externa del núcleo. Se utiliza este diseño porque un rayo de luz que sigue un modo que pasa

directamente por el centro del núcleo no viaja tanto como un rayo que sigue un modo que rebota en la fibra. Todos los rayos deberían llegar al extremo opuesto de la fibra al mismo tiempo. Entonces, el receptor que se encuentra en el extremo de la fibra, recibe un fuerte flash de luz y no un pulso largo y débil.

Alrededor del núcleo se encuentra el revestimiento. El revestimiento también está fabricado con sílice pero con un índice de refracción menor que el del núcleo. Los rayos de luz que se transportan a través del núcleo de la fibra se reflejan sobre el límite entre el núcleo y el revestimiento a medida que se mueven a través de la fibra por reflexión total interna.

El cable de fibra óptica multimodo estándar es el tipo de cable de fibra óptica que más se utiliza en las LAN. Un cable de fibra óptica multimodo estándar utiliza una fibra óptica con núcleo de 62,5 ó 50 micrones y un revestimiento de 125 micrones de diámetro. A menudo, recibe el nombre de fibra óptica de 62,5/125 ó 50/125 micrones. Un micrón es la millonésima parte de un metro (1µ).

Alrededor del revestimiento se encuentra un material amortiguador que es generalmente de plástico. El material amortiguador ayuda a proteger al núcleo y al revestimiento de cualquier daño.

Existen dos diseños básicos para cable. Son los diseños de cable de amortiguación estrecha y de tubo libre. La mayoría de las fibras utilizadas en la redes LAN son de cable multimodo con amortiguación estrecha. Los cables con amortiguación estrecha tienen material amortiguador que rodea y está en contacto directo con el revestimiento.

La diferencia más práctica entre los dos diseños está en su aplicación. El cable de tubo suelto se utiliza principalmente para instalaciones en el exterior de los edificios mientras que el cable de amortiguación estrecha se utiliza en el interior de los edificios.

El material resistente rodea al amortiguador, evitando que el cable de fibra óptica se estire cuando los encargados de la instalación tiran de él. El material utilizado es, en general, Kevlar, el mismo material que se utiliza para fabricar los chalecos a prueba de bala.

El último elemento es el revestimiento exterior. El revestimiento exterior rodea al cable para así proteger la fibra de abrasión, solventes y demás contaminantes. El color del revestimiento exterior de la fibra multimodo es, en general, anaranjado, pero a veces es de otro color.

Los Diodos de Emisión de Luz Infrarroja (LED) o los Emisores de Láser de Superficie de Cavidad Vertical (VCSEL) son dos tipos de fuentes de luz utilizadas normalmente con fibra multimodo. Se puede utilizar cualquiera de los dos. Los LED son un poco más económicos de fabricar y no requieren tantas normas de seguridad como los láseres. Sin embargo, los LED no pueden transmitir luz por un cable a tanta distancia como el láser. La fibra multimodo (62,5/125) puede transportar datos a distancias de hasta 2000 metros (6.560 pies).

1.3.7 Fibra Monomodo

La fibra monomodo consta de las mismas partes que una multimodo. El revestimiento exterior de la fibra monomodo es, en general, de color amarillo. La mayor diferencia entre la fibra monomodo y la multimodo es que la monomodo permite que un solo modo de luz se propague a través del núcleo de menor diámetro de la fibra óptica. El núcleo de una fibra monomodo tiene de ocho a diez micrones de diámetro. Los más comunes son los núcleos de nueve micrones.

La marca 9/125 que aparece en el revestimiento de la fibra monomodo indica que el núcleo de la fibra tiene un diámetro de 9 micrones y que el revestimiento que lo envuelve tiene 125 micrones de diámetro.

En una fibra monomodo se utiliza un láser infrarrojo como fuente de luz. El rayo de luz que el láser genera, ingresa al núcleo en un ángulo de 90 grados.

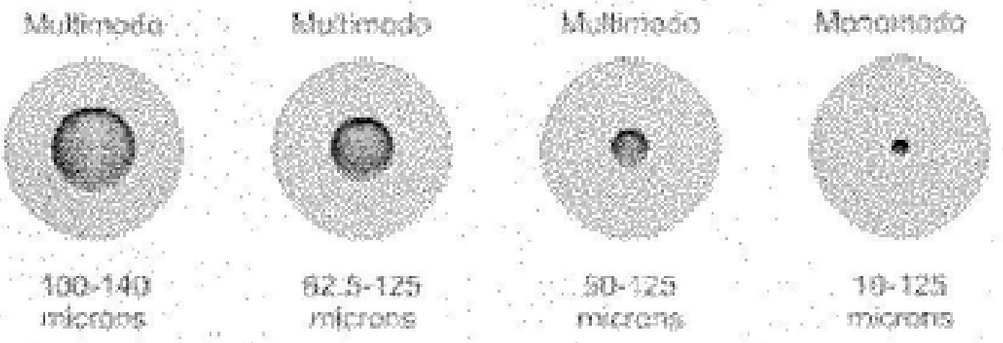
Como consecuencia, los rayos de luz que transportan datos en una fibra monomodo son básicamente transmitidos en línea recta directamente por el centro del núcleo.

Esto aumenta, en gran medida, tanto la velocidad como la distancia a la que se pueden transmitir los datos.

Por su diseño, la fibra monomodo puede transmitir datos a mayores velocidades (ancho de banda) y recorrer mayores distancias de tendido de cable que la fibra multimodo. La fibra monomodo puede transportar datos de LAN a una distancia de hasta 3000 metros. Aunque está distancia se considera un estándar, nuevas tecnologías han incrementado esta distancia y serán discutidas en un módulo posterior.

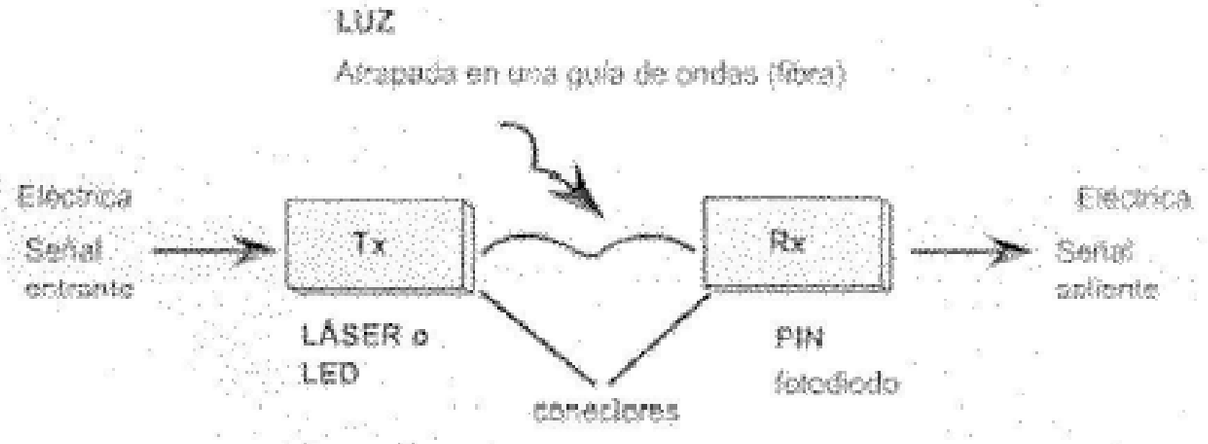
La fibra multimodo sólo puede transportar datos hasta una distancia de 2000 metros. Las fibras monomodo y el láser son más costosos que los LED y la fibra multimodo. Debido a estas características, la fibra monomodo es la que se usa con mayor frecuencia para la conectividad entre edificios.

La Figura compara los tamaños relativos del núcleo y el revestimiento para ambos tipos de fibra óptica en distintos cortes transversales. Como la fibra monomodo tiene un núcleo más refinado y de diámetro mucho menor, tiene mayor ancho de banda y distancia de tendido de cable que la fibra multimodo. Sin embargo, tiene mayores costos de fabricación.



1.3.6 Otros Componentes Ópticos

La mayoría de los datos que se envían por una LAN se envían en forma de señales eléctricas. Sin embargo, los enlaces de fibra óptica utilizan luz para enviar datos. Hace falta algún elemento para convertir la electricidad en luz y, en el otro extremo de la fibra, para convertir la luz nuevamente en electricidad. Esto significa que se requiere un transmisor y un receptor.



El transmisor recibe los datos que se deben transmitir desde los switches y routers. Estos datos tienen forma de señales eléctricas. El transmisor convierte las señales electrónicas en pulsos de luz equivalentes. Existen dos tipos de fuentes de luz que se utilizan para codificar y transmitir los datos a través del cable:

- Un diodo emisor de luz (LED) que produce luz infrarroja con longitudes de onda de 850 nm o 1310 nm. Se utilizan con fibra multimodo en las LAN. Para enfocar la luz infrarroja en el extremo de la fibra, se utilizan lentes.
- Amplificación de la luz por radiación por emisión estimulada (LASER) una fuente de luz que produce un fino haz de intensa luz infrarroja, generalmente, con longitudes de onda de 1310nm o 1550 nm. Los láser se usan con fibra monomodo para las grandes distancias de los backbones de universidades y WAN. Se debe tener sumo cuidado a fin de evitar daños a la vista.

Cada una de estas fuentes de luz puede ser encendida y apagada muy rápidamente para así enviar datos (unos y ceros) a un elevado número de bits por segundo.

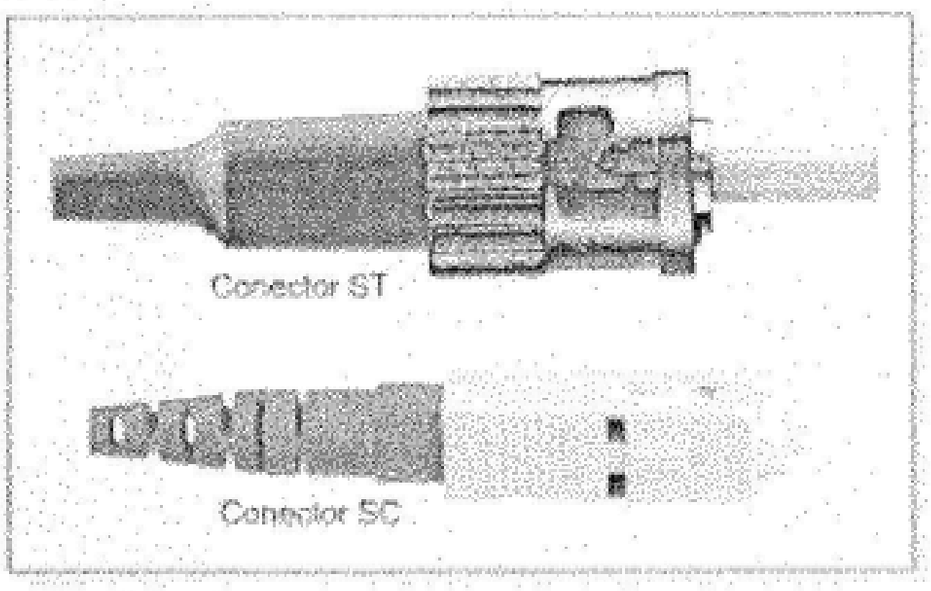
En el otro extremo de la fibra óptica conectada al transmisor se encuentra el receptor. El receptor funciona casi como una célula fotoeléctrica en una calculadora a energía solar.

Cuando la luz llega al receptor, se genera electricidad. La primera tarea del receptor es detectar el pulso de luz que llega desde la fibra. Luego, el receptor convierte el pulso de luz nuevamente en la señal eléctrica original tal como ingresó al transmisor al otro extremo de la fibra. Ahora, la señal nuevamente adquiere la forma de cambios de voltaje.

La señal está lista para ser enviada por el cable de cobre al dispositivo electrónico receptor, como por ejemplo, un computador, switch o router. Los dispositivos semiconductores que se utilizan generalmente como receptores con enlaces de fibra óptica reciben el nombre de diodos p-intrínsecos–n (fotodiodos PIN).

Los fotodiodos PIN están fabricados para ser sensibles a 850; 1310 ó 1550 nm de luz que el transmisor genera al otro extremo de la fibra. Cuando un pulso de luz de la longitud de onda adecuada da en el fotodiodo PIN, éste rápidamente genera una corriente eléctrica de voltaje apropiado para la red. Cuando la luz deja de iluminar el fotodiodo PIN, éste deja de generar voltaje al instante. Esto genera cambios de voltaje que representan los unos y ceros de los datos en el cable de cobre.

Hay conectores unidos a los extremos de las fibras de modo que éstas puedan estar conectadas a los puertos del transmisor y del receptor. El tipo de conector que se usa con mayor frecuencia con la fibra multimodo es el Conector Suscriptor (conector SC). En una fibra monomodo, el conector de Punta Recta (ST) es el más frecuentemente utilizado.



Además de los transmisores, receptores, conectores y fibras que siempre son necesarios en una red óptica, a menudo también se ven repetidores y paneles de conexión de fibra.

Los repetidores son amplificadores ópticos que reciben pulsos de luz atenuante que recorren largas distancias y los convierte a su forma, fuerza y sincronización originales. Las señales restauradas pueden entonces enviarse hasta el receptor que se encuentra en el extremo final de la fibra.

Los paneles de conexión de fibra son similares a los paneles de conexión que se usan con el cable de cobre. Estos paneles aumentan la flexibilidad de una red óptica permitiendo que se realicen rápidos cambios en la conexión de los dispositivos, como por ejemplo, switches o routers con distintos tendidos de fibra o enlaces de cable disponibles.

Aunque la fibra es el mejor de todos los medios de transmisión a la hora de transportar grandes cantidades de datos a grandes distancias, la fibra también presenta dificultades. Cuando la luz viaja a través de la fibra, se pierde parte de la energía de la luz. Cuanto mayor es la distancia a la que se envía una señal a través de una fibra, más fuerza pierde la señal.

Esta atenuación de la señal se debe a diversos factores implícitos en la naturaleza de la fibra en sí. El factor más importante es la dispersión. La dispersión de la luz dentro de una fibra es producida por defectos microscópicos en la uniformidad (distorsiones) de la fibra que reflejan y dispersan parte de la energía de la luz.

La absorción es otra causa de pérdida de la energía de la luz. Cuando un rayo de luz choca algunos tipos de impurezas químicas dentro de una fibra, estas impurezas absorben parte de la energía. Esta energía de la luz se convierte en

una pequeña cantidad de energía calórica. La absorción hace que la señal luminosa sea un poco más débil.

Otro factor que causa atenuación en la señal luminosa son las irregularidades o asperezas de fabricación en el límite entre el núcleo y el revestimiento. Se pierde potencia en la señal luminosa debido a que la reflexión interna total no es perfecta en el área áspera de la fibra. Cualquier imperfección microscópica en el espesor o simetría de la fibra reducirá la reflexión interna total y el revestimiento absorberá parte de la energía de la luz.

La dispersión de un destello de luz también limita las distancias de transmisión de una fibra. Dispersión es el término técnico para la difusión de los pulsos de luz a medida que viajan a través de la fibra.

1.3.9 Instalación, Cuidado Y Prueba De La Fibra Óptica

Una de las causas principales de la atenuación excesiva en el cable de fibra óptica es la instalación incorrecta. Si se estira o curva demasiado la fibra, se pueden producir pequeñas fisuras en el núcleo que dispersan los rayos de luz.

Para evitar que la curvatura de la fibra sea demasiado pronunciada, generalmente, se introduce la fibra a un tipo de tubo instalado que se llama de interducto.

El interducto es mucho más rígido que la fibra y no se puede curvar de forma pronunciada, de modo que la fibra en el interducto tampoco puede curvarse en exceso. El interducto protege la fibra, hace que sea mucho más sencillo el tendido y asegura que no se exceda el radio de la curvatura (límite de curva) de la fibra.

Una vez que el cable de fibra óptica y los conectores han sido instalados, los conectores y los extremos de las fibras deben mantenerse totalmente limpios. Los extremos de las fibras deben cubrirse con cubiertas protectoras para evitar daños. Cuando estas cubiertas son retiradas, antes de conectar la fibra a un puerto en un switch o router, se deben limpiar los extremos de las fibras. Se deben limpiar los extremos de la fibra con paño especial sin pelusa para limpiar lentes, humedecido con alcohol isopropílico puro.

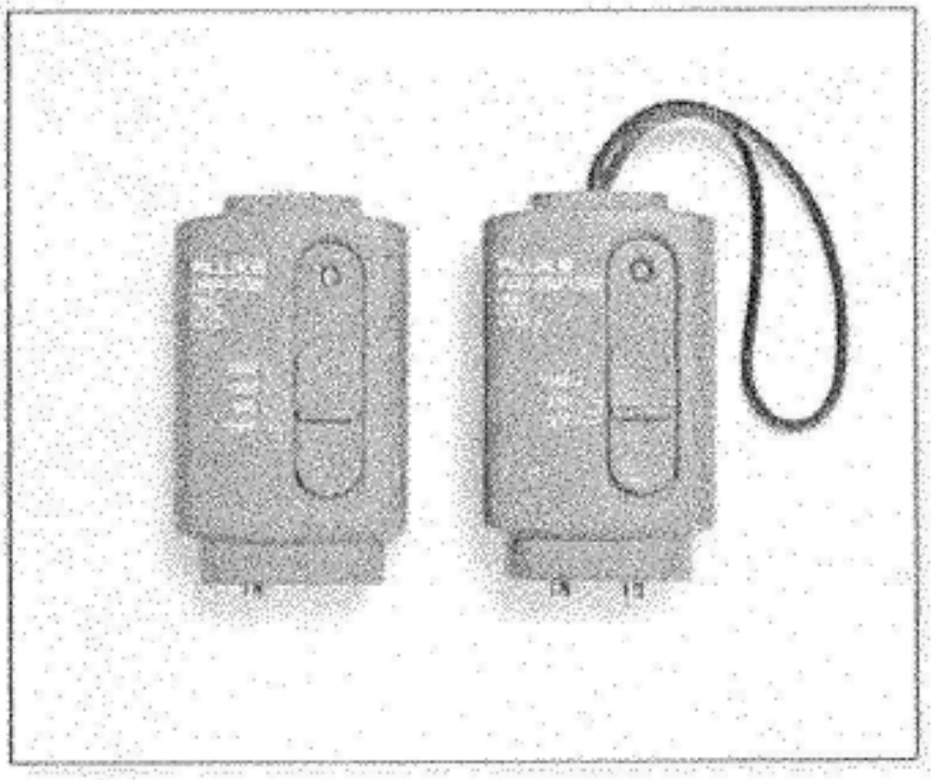
Los puertos de fibra de un switch o router también deben mantenerse cubiertos cuando no se encuentran en uso y limpiarse con paño especial para limpiar lentes y alcohol isopropílico antes de realizar la conexión. La suciedad en los extremos de una fibra disminuirá gravemente la cantidad de luz que llega al receptor.

La dispersión, absorción, difusión, incorrecta instalación y los extremos de fibra sucios son factores que disminuyen la fuerza de la señal luminosa y se conocen como ruido de fibra. Antes de usar un cable de fibra óptica, es importante probarlo para asegurarse de que suficiente luz llegue al receptor para que éste pueda detectar los ceros y los unos en la señal.

Al planear un enlace de fibra óptica, es necesario calcular la pérdida tolerable de la potencia de la señal. Esto se conoce como presupuesto de pérdida del enlace óptico. Piense en un presupuesto financiero mensual. Una vez que todos los gastos son sustraídos del ingreso inicial, debe quedar dinero suficiente para todo el mes.

El decibel (dB) es la unidad utilizada para medir la cantidad de pérdida de potencia. Mide el porcentaje de potencia que sale del transmisor y realmente llega al receptor.

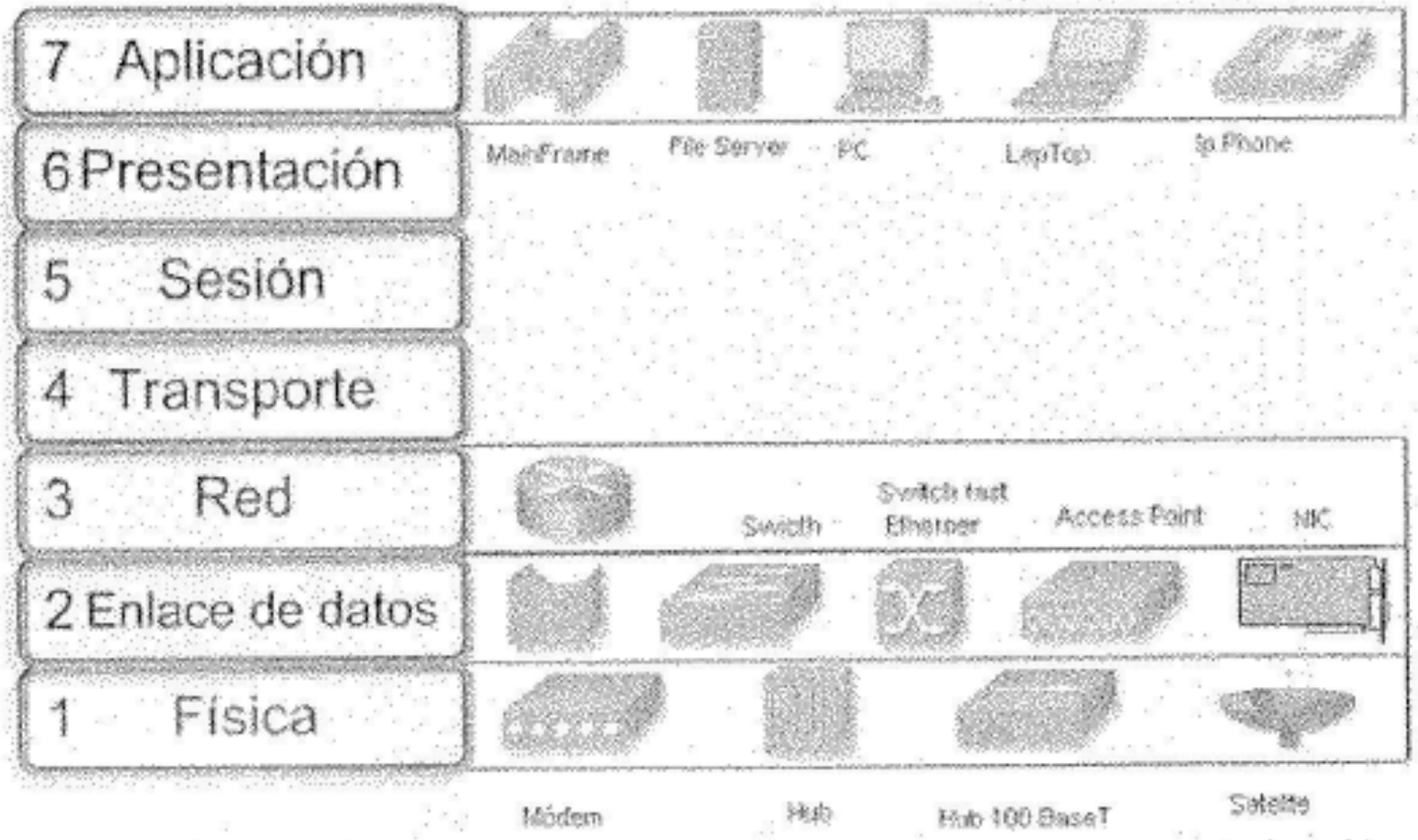
Es de suma importancia probar los enlaces de fibra y se deben mantener registros de los resultados de estas pruebas. Se utilizan varios tipos de equipo de prueba para fibra óptica. Dos de los instrumentos más importantes son los Medidores de Pérdida Óptica y los Reflectómetros Ópticos de Dominio de Tiempo (OTDR).



Estos medidores prueban el cable óptico para asegurar que el cable cumpla con los estándares TIA para la fibra. También verifican que la pérdida de potencia del enlace no caiga por debajo del presupuesto de pérdida del enlace óptico. Los

OTDR pueden brindar mucha información detallada de diagnóstico sobre el enlace de fibra. Pueden utilizarse para detectar las fallas de un enlace cuando se produce un problema

1.4 DISPOSITIVOS DE LAS DIFERENTES CAPAS



1.5 CAPA FÍSICA DE LA LAN

Ethernet es la tecnología LAN de uso más frecuente. Un grupo formado por las empresas Digital, Intel y Xerox, conocido como DIX, fue el primero en implementar Ethernet. DIX creó e implementó la primera especificación LAN Ethernet, la cual se utilizó como base para la especificación 802.3 del Instituto de Ingenieros Eléctrica y Electrónica (IEEE), publicada en 1980. Más tarde, el IEEE extendió la especificación 802.3 a tres nuevas comisiones conocidas como 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet transmitido en fibra óptica) y 802.3ab (Gigabit Ethernet en UTP).

Los requisitos de la red pueden forzar a la actualización a topologías de Ethernet más rápidas. La mayoría de las redes de Ethernet admiten velocidades de 10 Mbps y 100 Mbps

La nueva generación de productos para multimedia, imagen y base de datos puede fácilmente abrumar a redes que funcionan a las velocidades tradicionales

de Ethernet de 10 y 100 Mbps. Los administradores de red pueden considerar proveer Gigabit Ethernet desde el backbone hasta los usuarios finales.

Los costos de instalación de un nuevo cableado y de adaptadores pueden hacer que esto resulte casi imposible. Por el momento, Gigabit Ethernet en el escritorio no constituye una instalación estándar.

Por lo general, las tecnologías Ethernet se pueden utilizar en redes de campus de muchas maneras diferentes:

- Se puede utilizar Ethernet de 10 Mbps a nivel del usuario para brindar un buen rendimiento. Los clientes o servidores que requieren mayor ancho de banda pueden utilizar Ethernet de 100-Mbps.
- Se usa Fast Ethernet como enlace entre el usuario y los dispositivos de red. Puede admitir la combinación de todo el tráfico de cada segmento Ethernet.
- Para mejorar el rendimiento cliente-servidor a través de la red campus y evitar los cuellos de botella, se puede utilizar Fast Ethernet para conectar servidores empresariales.
- A medida que se tornen económicos, se debe implementar Fast Ethernet o Gigabit Ethernet entre dispositivos backbone.

1.5.1 Cables De Fibras Ópticas Para Redes Lan

La elección del conductor de fibra óptica depende del sistema, es decir los correspondientes diodos emisores y receptores. Por lo tanto, lo único específico en estos cables es el diámetro del núcleo del conductor de fibra óptica; todos los demás elementos constitutivos del cable se utilizan según el uso previsto (instalación interior y/o exterior). Valores habituales para el diámetro del núcleo/recubrimiento son 50/125 µ m, 62,5/125 µ m, así como 85/125 µ m y 100/140 µ m. De la capa protectora aplicada encima del núcleo y recubrimiento resultan diámetros de 250 y 500 µ m, respectivamente.

Para las vías de transmisión de banda ancha son apropiados los cables de fibras ópticas, pues con ellos es posible realizar sistemas con velocidades de transmisión de hasta unos 100 Mbit/s y distancias de hasta 10 Km. sin regenerador.

1.6 SERVIDOR DE DHCP

DHCP (sigla en inglés de **Dynamic Host Configuration Protocol**) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en

el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido y a quien se la ha asignado después.

1.6.1 Características

Provee los parámetros de configuración a las computadoras conectadas a la red informática que lo requieran (máscara, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

El protocolo DHCP es muy utilizado en la administración de redes, ya que permite que los equipos configuren automáticamente los parámetros de red (dirección IP, máscara de red, dirección de difusión, encaminador por defecto, servidor de nombres).

Otras características de DHCP son:

- Administración más sencilla.
- Configuración automatizada.
- Permite cambios y traslados.
- Posibilidad de que el cliente solicite los valores de ciertos parámetros.
- Nuevos tipos de mensajes de DHCP que soportan interacciones cliente/servidor robustas.

1.6.2 Ventajas Del Uso De DHCP

DHCP proporciona las siguientes ventajas de administración en una red TCP/IP:

- **Configuración segura y confiable.**

DHCP evita los errores de configuración que se producen por la necesidad de escribir los valores manualmente en cada equipo. Así mismo, DHCP ayuda a evitar los conflictos de direcciones que se producen al configurar un equipo nuevo en la red con una dirección IP ya asignada.

- **Reduce la administración de la configuración.**

La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y modificar la configuración de los equipos de la red. Los servidores se pueden configurar para que suministren un conjunto completo de valores de configuración adicionales al asignar concesiones de direcciones. Estos valores se asignan mediante opciones DHCP.

Así mismo, el proceso de renovación de concesiones de DHCP ayuda a garantizar que en las situaciones en que sea necesario actualizar a menudo la configuración de los clientes (como en el caso de usuarios con equipos móviles o portátiles que cambian frecuentemente de ubicación), los clientes que se comunican directamente con los servidores DHCP puedan realizar estos cambios de forma eficaz y automática.

1.6.3 Asignación De Direcciones IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual**: donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.

- **Asignación automática**: donde una dirección de IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.

- **Asignación dinámica**: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el DNS asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS.

1.6.4 Motivos Para Usar El Protocolo DHCP

DHCP es útil para proporcionar de un modo rápido la configuración de red del cliente. Al configurar el sistema cliente, el administrador puede seleccionar el

protocolo DHCP y no especificar una dirección IP, una máscara de red, un gateway o servidor DNS. El cliente recupera esta información desde el servidor DHCP. DHCP también es útil si un administrador desea cambiar la dirección de IP de muchos sistemas. En lugar de volver a configurar todos los sistemas, puede modificar un fichero de configuración DHCP en el servidor para establecer la nueva dirección IP. Si los servidores DNS de una organización cambian, los cambios también se aplicarán en el servidor DHCP, no en todos los clientes DHCP. Una vez que se reinicie la red en los clientes (o rearranquen los clientes), se aplicarán los cambios.

Además, si un portátil o cualquier tipo de equipo móvil se configuran para DHCP, podrá desplazarse entre distintas oficinas sin tener que volver a configurarlo, ya que cada oficina dispondrá de un servidor DHCP que permitirá su conexión a la red.

1.6.5 Funcionamiento Del Servidor DHCP

La configuración de DHCP se basa en un fichero de texto, **/etc/dhcp.conf** que el proceso servidor lee en el inicio. La lectura del fichero de configuración sólo se realiza durante el inicio, nunca cuando ya está en ejecución, por tanto cualquier modificación requiere detener el servicio DHCP y volverlo a iniciar. En este fichero se especifican las características de comportamiento como son el rango de direcciones asignadas, el tiempo de asignación de direcciones, el nombre del dominio, los gateways, etc. DHCP almacena en memoria la lista de direcciones de cada subred que está sirviendo. Cuando se arranca un cliente DHCP le solicita una dirección al servidor, éste busca una dirección disponible y se la asigna. En caso de necesidad, el servidor DHCP también puede asignar direcciones fijas a determinados equipos de la red.

1.6.6 Parámetros Configurables

Un servidor puede proveer de una configuración opcional a la computadora cliente.

Lista de opciones configurables:

- Dirección del servidor **DNS**
- Nombre **DNS**
- Puerta de enlace de la dirección IP
- Máscara de subred.
- Distribución de **ARP** (**Protocolo de Resolución de Direcciones** según siglas en inglés).

- Servicio **FTP (File Transfer Protocol)**.
- Servicio de **PROXY.**
- Servicio de **FIREWALL.**

La asignación de los datos TCP/IP al cliente se realiza para un determinado espacio de tiempo que se define en la configuración del servidor. Si no se especifica otro valor, la asignación predeterminada es por un día. También los clientes pueden solicitar datos de una duración especificada, aunque para evitar que un cliente tenga una dirección fija se puede prefijar un tiempo máximo de asignación.

Si tenemos varias subredes en nuestra instalación, también se pueden diferenciar las asignaciones que otorga el servidor DHCP según el interfaz en el que se realice.

Como el servidor DHCP puede pararse y reiniciarse, necesita mantener la lista de direcciones asignadas. El fichero **/var/lib/dhcp/dhcpd.leases** o **/var/state/dhcp/dhcpd**.leases mantiene esta lista de asignaciones. Cuando se inicia el servidor, primero lee el fichero de configuración dhcpd.conf, después el fichero dhcpd.leases y marca qué sistemas tienen asignaciones activas.

1.6.7 El Servidor DNS

Todos los ordenadores que utilizan el protocolo IP tienen al menos una dirección IP, que debe ser única dentro de la red a la que pertenecen. En Internet hay una serie de organizaciones como InterNIC, que asignan las direcciones IP. A cada dirección IP se le puede asignar un nombre, que debe ser único. El mecanismo para obtener la dirección IP a partir del nombre se le llama "resolución del nombre". Además a cada dirección IP se le puede asignar otros nombres, conocidos como alias.

El sistema más sencillo para resolver los nombres dentro del protocolo TCP/IP es el archivo HOST. Este archivo contiene entradas del tipo dirección IP y nombre, que permiten resolver el nombre de un servidor. Si la red es pequeña es fácil distribuir el fichero de HOST entre los servidores. Este método suele ser soportado por la mayoria de las pilas TCP/IP disponibles, aunque el mecanismo de resolución de nombres preferido para las redes grandes como Internet es el DNS.

1.6.7.1 Historia Del DNS

En la década de los 70, la red Arpanet, antecesora de Internet, estaba formada por un número pequeño de servidores. En un sencillo archivo **HOST.TXT** figuraban los

pocos centenares de servidores que la componían. Para realizar cambios en este fichero, los administradores de los diferentes servidores enviaban las modificaciones por correo electrónico y recibían el nuevo fichero **HOST.TXT** actualizado por FTP. El organismo encargado de mantener el fichero era **SRINIC**. Con el crecimiento de Arpanet la capacidad de **NIC** para mantener el fichero original se vio desbordada. Además apareció el problema de servidores con nombre duplicado. En 1984 se creó el sistema de nombres de dominio DNS (**Domain Name System**), documentado en las RFC 882 y 883.

1.6.8 Puerta De Enlace

Una **puerta de enlace** o **gateway** es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: **Network Address Translation**). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada **IP Masquerading** (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Se podría decir que un gateway, o puerta de enlace, es un router que conecta dos redes. La dirección IP De un gateway (o puerta de enlace) a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza Algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x, que engloban o se reservan a las redes locales. (Además se debe notar que necesariamente un equipo que haga de puerta de enlace en una red, debe tener 2 tarjetas de red.

1.6.9 Máscara De Red

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Sirve para que un ordenador (principalmente la puerta de enlace, router, etc.) sepa si debe enviar los datos dentro o fuera de la red. Es decir, la función de la máscara de red es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host. Por ejemplo, si el router tiene la IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras IPS, para fuera (Internet, otra red local).

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. También se puede escribir como 10.0.0.0/8

Como la máscara consiste en una secuencia de puros unos seguidos por puros ceros, los números permitidos para representar la secuencia son los siguientes: 0, 128, 192, 224, 240, 248, 252, 254, y 255.

La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de red representada en binario son 4 octetos de bits (11111111.11111111.11111111.11111111).

1.6.10 Protocolo ARP

ARP son las siglas en inglés de **Address Resolution Protocol** (Protocolo de resolución de direcciones).

Es un protocolo de nivel de red responsable de encontrar la dirección hardware (**Ethernet MAC**) que corresponde a una determinada dirección IP. Para ello se envía un paquete (**ARP request**) a la dirección de multidifusión de la red (**broadcast** (**MAC = ff ff ff ff ff ff**)) conteniendo la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (**ARP reply**) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto solo funciona si todas las máquinas lo soportan.

El protocolo **RARP** realiza la operación inversa.

En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

1. Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.

2. Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
3. Cuando un router necesita enviar un paquete a un host a través de otro router.
4. Cuando un router necesita enviar un paquete a un host de la misma red.

1.6.10.1 Tablas ARP

La filosofía es la misma que tendríamos para localizar al señor X entre 150 personas: preguntar por su nombre a todo el mundo, y el señor X nos responderá. Así, cuando a A le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su frame ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física. En este momento A ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla)

1.6.11 Protocolo FTP

Es uno de los diversos protocolos de la red Internet, concretamente significa **File Transfer Protocol** (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red. Su comportamiento está definido por la recomendación RFC 959.

Se precisa de un Servidor **FTP** y un cliente **FTP**, puede darse el caso de que los servidores sean de libre acceso para todo el mundo y entonces estamos hablando de login anónimo o **FTP** anónimo.

La mayoría de las páginas web a nivel mundial son subidas a los respectivos servidores mediante este protocolo.

Por defecto utiliza los puertos 20 y 21. El puerto 20 es el utilizado para el flujo de datos entre el cliente y el servidor y el puerto 21 para el flujo de control, es decir, para enviar las órdenes del cliente al servidor. Mientras se transfieren datos a través del flujo de datos, el flujo de control permanece en espera. Esto puede causar problemas en el caso de transferencias de datos muy grandes realizadas a través de cortafuegos que interrumpan sesiones después de periodos largos en espera. El archivo puede que se haya transferido con éxito, pero el cortafuegos puede desconectar la sesión de control, por lo que se genera un error.

También se puede utilizar el protocolo FTP utilizando un navegador web con una dirección del tipo ftp://*usuario:contraseña@servidor*, por ejemplo: ftp://usulec:clavel@archivos.miempresa.com

Puede emplearse wget. Este programa recibe un URL y puede descargarlo así como todos los documentos que este enlace (y los que los documentos enlazados enlacen de forma recursiva).

1.6.11.1 Introducción a File Transfer Protocol (FTP):

Existe en la actualidad, dentro de lo que es Internet, un 'servicio' que permite trabajar con archivos (copiar, modificar, borrar) desde una PC hacia un servidor remoto. En dichos servidores remotos se alojan grandes cantidades de **shareware** y **freeware**, que están a disposición del público para que haga un download a su computadora. Generalmente estos servidores permiten el acceso a cualquier usuario (servidores llamados **"anonymous"**) pero también existen los servidores que tienen acceso restringido por medio de passwords o contraseñas.

Estas transferencias de archivos se hacen por medio de un software conocido como **FTP** (del inglés, **File Transfer Protocol**). Existen hoy en día muchos programas de este tipo, con diferentes prestaciones.

1.6.11.2 Algunas Definiciones FTP:

Abajo encontrará una lista con los términos más comunes en el uso de FTP:

- **Download:** Copiar un archivo desde una computadora remota (FTP site, server) a su computadora.
- **Upload:** Copiar un archivo desde su computadora a una computadora remota (FTP site, server).
- **Server**: Es como se llama comúnmente a un FTP site.

- **Session Profile**: Es el conjunto de información necesaria para conectarse a un server.

Hay tres datos importantes que Usted debe saber para conectarse a un Server FTP y bajar un programa a su computadora:

- El nombre del Host (ej.: www.ba.net).
- La ubicación del archivo, dentro de que directorio se encuentra (ej.: /pub/windows31).
- El nombre del archivo (ej.: n16e30.exe).

1.6.12 PROXY

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (por. ej: una página web) en una cache que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

1.6.12.1 Ventajas

En general (no sólo en informática), los proxies hacen posibles varias cosas nuevas:

- **Control**. Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

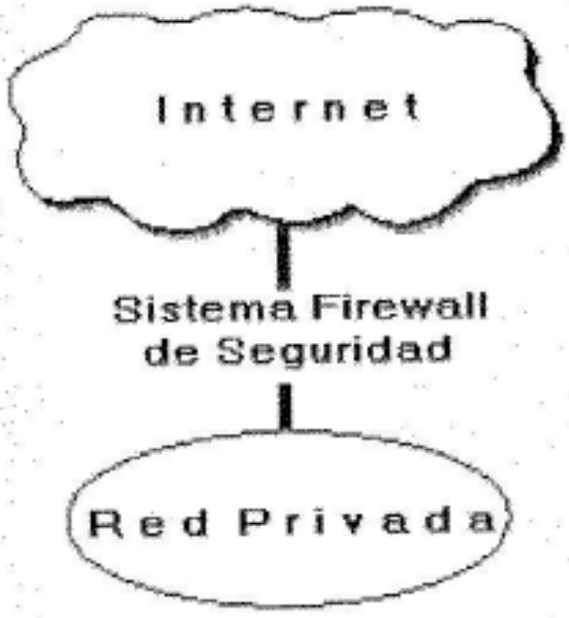
1.6.13 FIREWALL

Un **cortafuegos** (o **firewall** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un FIREWALL es el punto de conexión de la red interna de la organización con la red exterior, que

normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al FIREWALL una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un FIREWALL correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



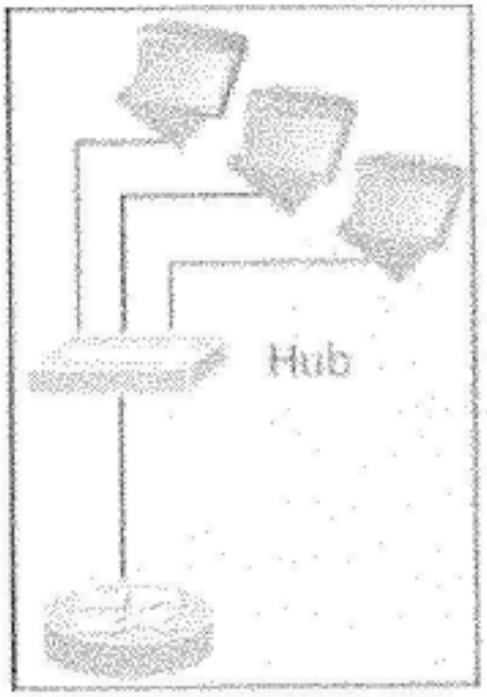
1.6.13.1 Ventajas De Un FIREWALL

- **Protege de intrusiones:** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- **Protección de información privada:** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- **Optimización de acceso:** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

1.7 VLANs

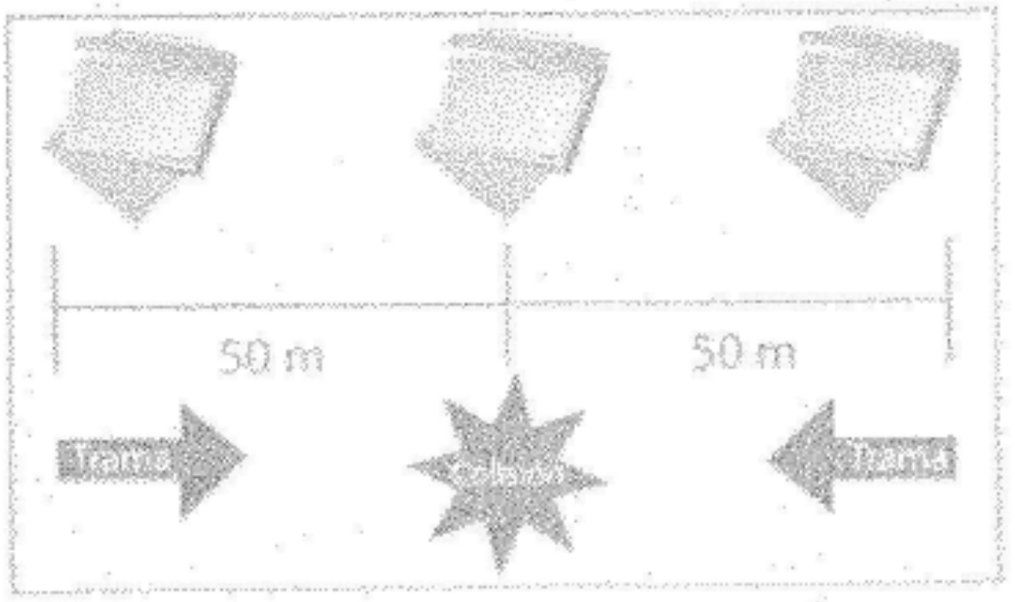
La característica principal de una red de área local es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma toman cierta cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de "tubería" se le puede llamar también "dominio de colisiones".



El empleo de un switch mejora el rendimiento de la red debido a que este dispositivo segmenta o divide los "dominios de colisiones", es decir, el comportamiento que se tiene en una LAN al utilizar concentradores o hubs es el de compartir el medio o ancho de banda, por ello puede ocurrir que en algún momento el medio esté ocupado por la transmisión de información por parte de alguna de las computadoras, y si otro quiere enviar información en esa precisa hora, no lo podrá hacer hasta que el medio se encuentre disponible.

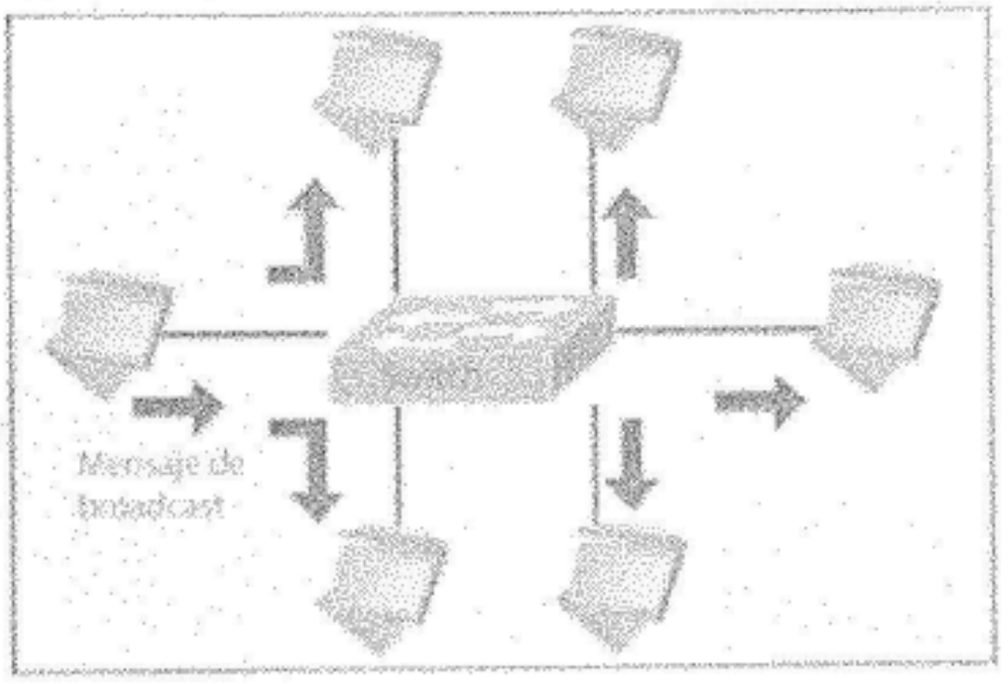
Por otro lado, si dos computadoras "escuchan" que el medio está vacío enviarán su información, pero debido a que éste es compartido puede suceder que los datos se encontrarán y "chocarán", por lo que se hablará de una colisión y el material se destruirá; al perderse tendrá que volverse a enviar, lo que llevará a muchas retransmisiones de información.



En una red LAN, cada uno de los puertos es una "tubería" dedicada a cada una de las casas (computadoras) dentro de la red, donde cada computadora dispone de toda la anchura de banda que la red proporciona, en este caso 10 o 100 Mbps, con objeto de evitar las colisiones que pudieran existir en un medio compartido, por ello cada computadora tiene un tubo individual enlazado con el punto central de distribución que es el switch.

Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de broadcast dentro de una red LAN, los que se asemejan a aquellos que escuchamos en una tienda departamental. Estos mensajes los escuchamos todos los que estamos en la tienda (la red LAN), ya sea que estén buscando a alguien o anunciando algún producto, y ninguna de las personas (computadoras) que estamos dentro de la tienda nos encontramos exentos de hacerlo.

En una LAN estos mensajes de broadcast son enviados a través de todos los puertos de un hub o de un switch. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además todas las computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del switch o concentrador.



Estos mensajes de broadcast son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de broadcast" o LAN.

Para solventar dicha situación se crea el concepto de Redes de Área Local Virtuales (VLANs), configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.
Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con los switchs, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los "dominios de colisión" por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los "dominios de broadcast", en lugar de uno solo, se puede configurar el switch para que existan más "dominios".
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.

- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán "vernos" como una Red de Área Local independiente a las demás.

El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

Hasta aquí ya hemos hablado de que se aísla el trafico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etcétera.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente.

1.7.1 Clases De VLAN

Como respuesta a los problemas generados en redes lan (colisiones, trafico broadcast, movilidad, etc) se creo una red con agrupamientos lógicos independientes del nivel físico, con lo cual si un usuario se encontraba en el piso uno y debía moverse al piso dos ya no tenia que reconfigurar la maquina ni darle una nueva dirección IP (Internet Protocol; Protocolo de Internet) del piso dos, sino que ahora era una acción automática.

Las VLAN (Virtual Local Area Networks; Redes virtuales de área local) forman grupos lógicos para definir los dominios de broadcast. De esta forma existe el dominio de los rojos, donde el broadcast que genera el rojo solo le afectara a este color y el broadcast que genera el amarillo solamente afectara a esta parte de la red.

Aunque físicamente estén conectadas las maquinas al mismo equipo, lógicamente pertenecerán a una VLAN distinta dependiendo de sus aplicaciones con lo que se logra un esquema mas enfocado al negocio.

Anteriormente existía la red plana, donde el broadcast se repetía en los puertos y esto provocaba una situación critica. Ahora con las VLAN existe una segmentación lógica o virtual.

Existen dos clases de VLAN: implícitas y explícitas. Las implícitas no necesitan cambios en el frame, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos. En esta clase de VLAN el usuario no modifica ni manipula el frame, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario.

Las VLAN explícitas si requieren modificaciones, adiciones y cambios (MAC) al frame, por lo que sacaron los estándares 802.1p y 802.1q, en donde se colocan ciertas etiquetas o banderas en el frame para manipularlo.

Las VLAN deben ser rápidas, basadas en switchs para que sean interoperables totalmente – porque los routers no dan la velocidad requerida- , su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.

1.7.2 Generaciones De VLAN

1. Basadas en puertos y direcciones MAC
2. Internet Working; se apoya en protocolo y dirección capa tres.
3. De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.
4. Servicios avanzados: ya se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host Configuration Protocol; Protocolo de configuración dinámica) o por AVLAN (Autenticate Virtual Local Area Networks; Redes virtuales autenticadas de área local).

1.7.3 VLAN Por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN - , el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN, por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla, el servidor estará en la VLAN amarilla.

1.7.4 VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación. Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

1.7.5 VLAN por Protocolo

Lo que pertenezca a IP sé enrutara a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectara automáticamente a la VLAN correspondiente.

1.7.6 VLAN Por Subredes De IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario aunque este conectado a la VLAN del protocolo IP sea asignado en otra VLAN subred que pertenecerá al grupo 10 o 20 dentro del protocolo.

1.7.7 VLAN Definidas Por El Usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario protocolo, dirección MAC y puerto. Si el usuario manifiesta otro patrón de bits, entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

1.7.8 VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente. También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

1.7.9 VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que

tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

1.8 PACKET SNIFFER

En informática, un **packet sniffer** es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta manera se puede obtener (sniffer) todo tipo de información de cualquier aparato conectado a la red como contraseñas, e-mails, conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por crackers, aunque también suelen ser usados para realizar comprobaciones y solucionar problemas en la red de modo legal).

1.8.1 Topología de red y packet sniffers

La cantidad de tramas que puede obtener un sniffer depende de la topología de red, del nodo donde esté instalado y del medio de transmisión. Por ejemplo:

- Para redes antiguas con topologías en estrella, el sniffer se podría instalar en cualquier nodo, ya que lo que hace el nodo central es retransmitir todo lo que recibe a todos los nodos. Sin embargo en las redes modernas, en las que solo lo retransmite al nodo destino, el único lugar donde se podría poner el sniffer para que capturara todas las tramas sería el nodo central.
- Para topologías en anillo, doble anillo y en bus, el sniffer se podría instalar en cualquier nodo, ya que todos tienen acceso al medio de transmisión compartido.
- Para las topologías en árbol, el nodo con acceso a más tramas sería el nodo raíz, aunque con los switches más modernos, las tramas entre niveles inferiores de un nodo viajarían directamente y no se propagarían al nodo raíz.

Es importante remarcar el hecho de que los sniffers sólo tienen efecto en redes que compartan el medio de transmisión como en redes sobre cable coaxial, cables de par trenzado (UTP, FTP o STP), o redes WiFi.

El uso de switch en lugar de hub incrementa la seguridad de la red ya que limita el uso de sniffers al dirigirse las tramas únicamente a sus correspondientes destinatarios.

1.8.2 Utilidad

Los principales usos que se le pueden dar son:

- Captura automática de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por hackers para atacar sistemas a posteriori.
- Conversión del tráfico de red en un formato entendible por los humanos.
- Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- Detección de intrusos, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados **IDS (Intrusión Detection System**, Sistema de Detección de intrusos), estos son prácticamente sniffers con funcionalidades específicas.
- Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.

2. ESTUDIO ACTUAL DE LA RED

2.1 DESCRIPCIÒN Y DISPOSITIVOS DE LA RED

La compañía BIOCHEM FARMACEUTICA actualmente posee una red con las siguientes características a nivel físico y lógico:

2.1.1 Dispositivos De Red:

- ROUTER CISCO 1720
  Velocidad 100 MBps,
  Ram 16mb
  Flash 4m
  Normas IEEE 802.3, IEEE 802.3U

- 3 SWITCH TRICOM DE 24 PUERTOS
  Velocidad 100/1000 MBPS

2.1.2 Dispositivos Hardware:

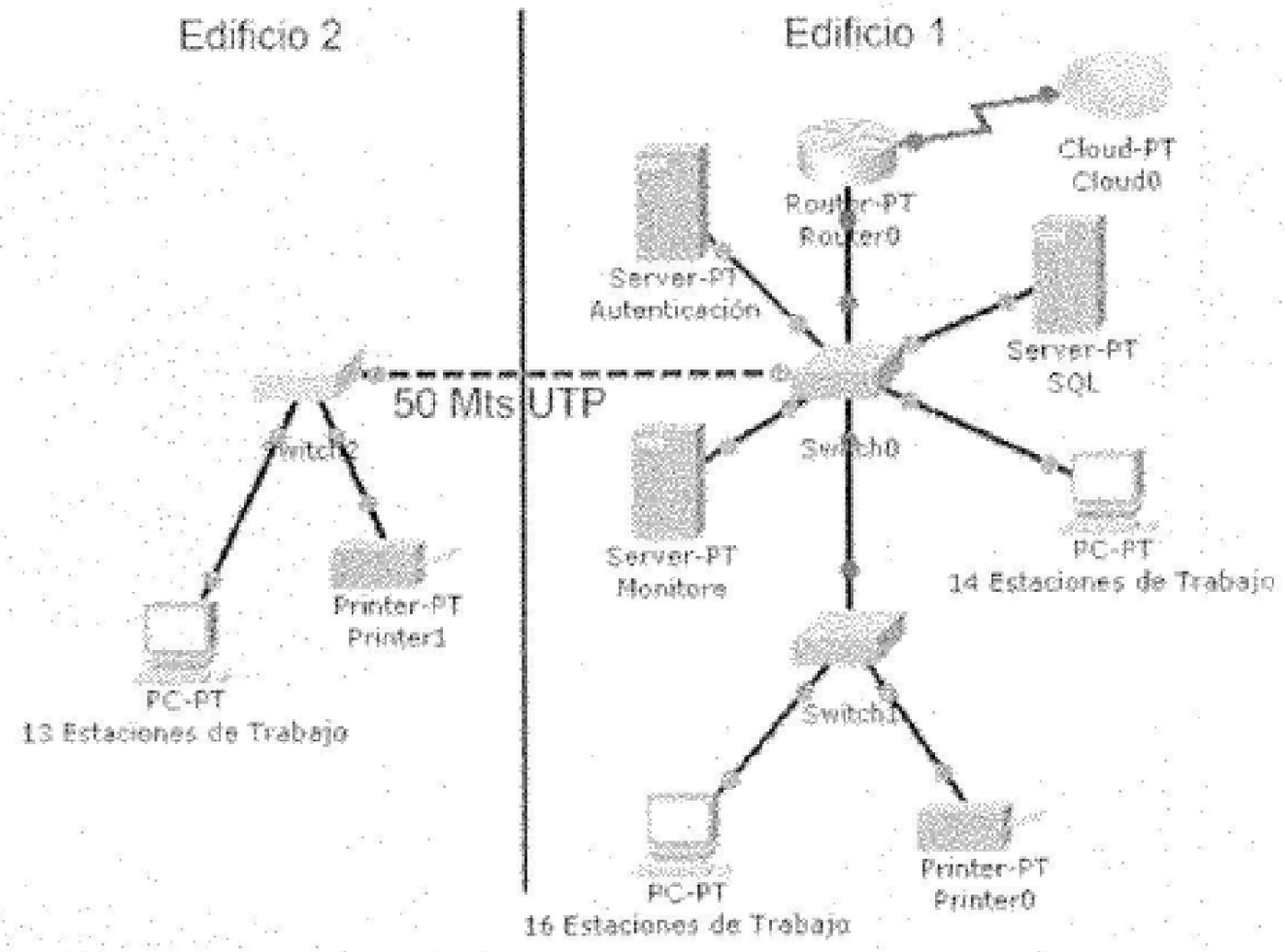
- Rack central.
- Pach Panel.
- 3 UPS 5 KW.
- Servidor Compaq ML370.
- Servidor HP ML370.
- 43 estaciones de trabajo.
- 16 genéricas.
- 20 Compaq.
- 7 Dell.

Actualmente la red de BIOCHEM FARMACUTICA cuenta con dos redes LAN ubicada cada una en un edificio. Las redes se interconectan entre si por medio de una conexión UTP de 50 m al mismo tiempo esto implica perdida del ancho de banda, por el cual el proveedor de servicios de Internet ofrece un ancho de banda de 1000k en fibra óptica y esta va directamente conectada a un ROUTER CISCO .

Además cuenta con tres servidores Compaq ML370 con Windows 2000 Server, uno para soporte de licencia de Office y aplicaciones de BIOSOFTWARE, otro para la autenticación de usuarios, el siguiente para la implementación de base de

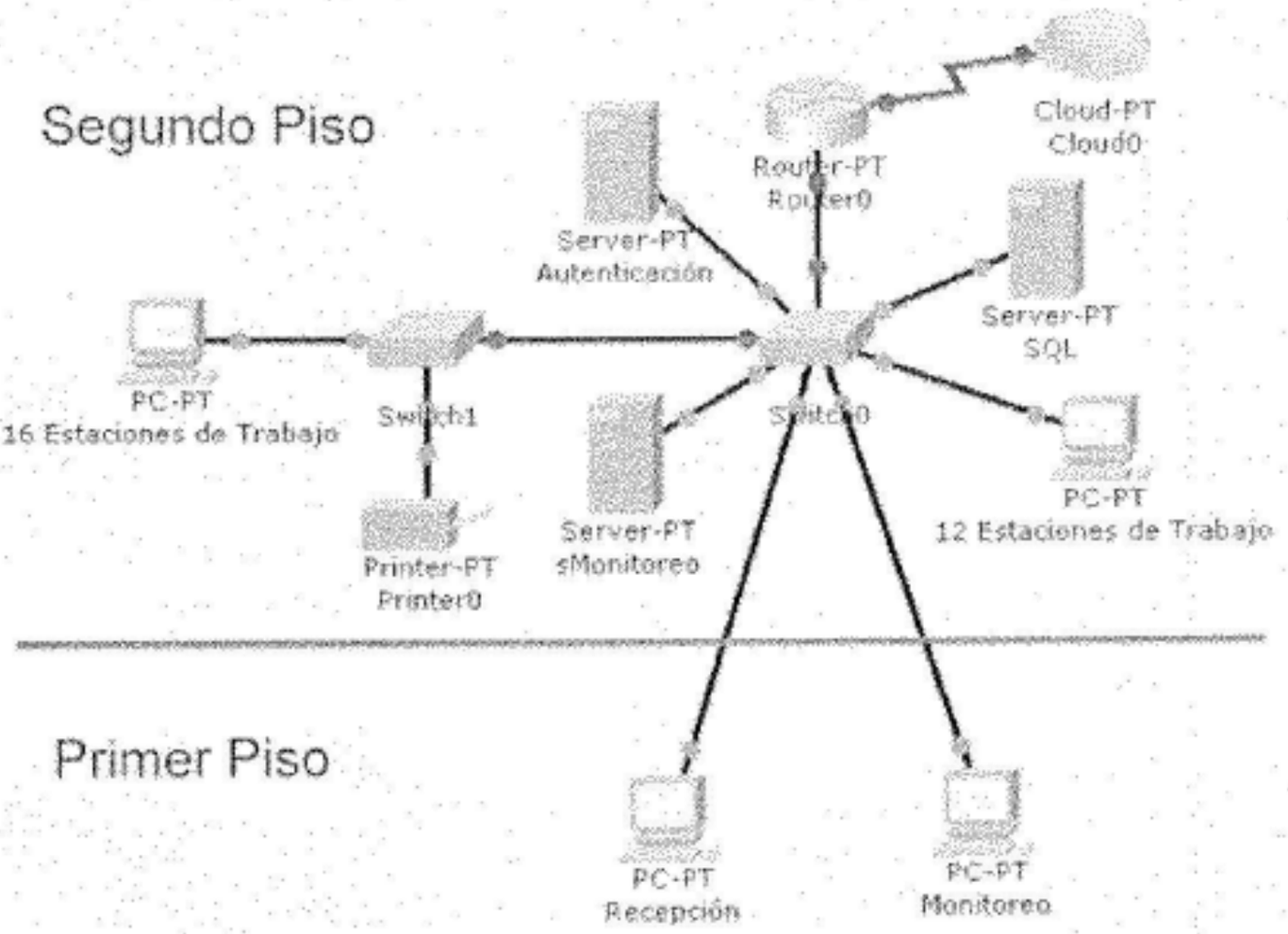
datos en SQL y otro para la administración de monitoreo de cámaras para la seguridad de la entidad.

Esquema Grafico lógico de la red.

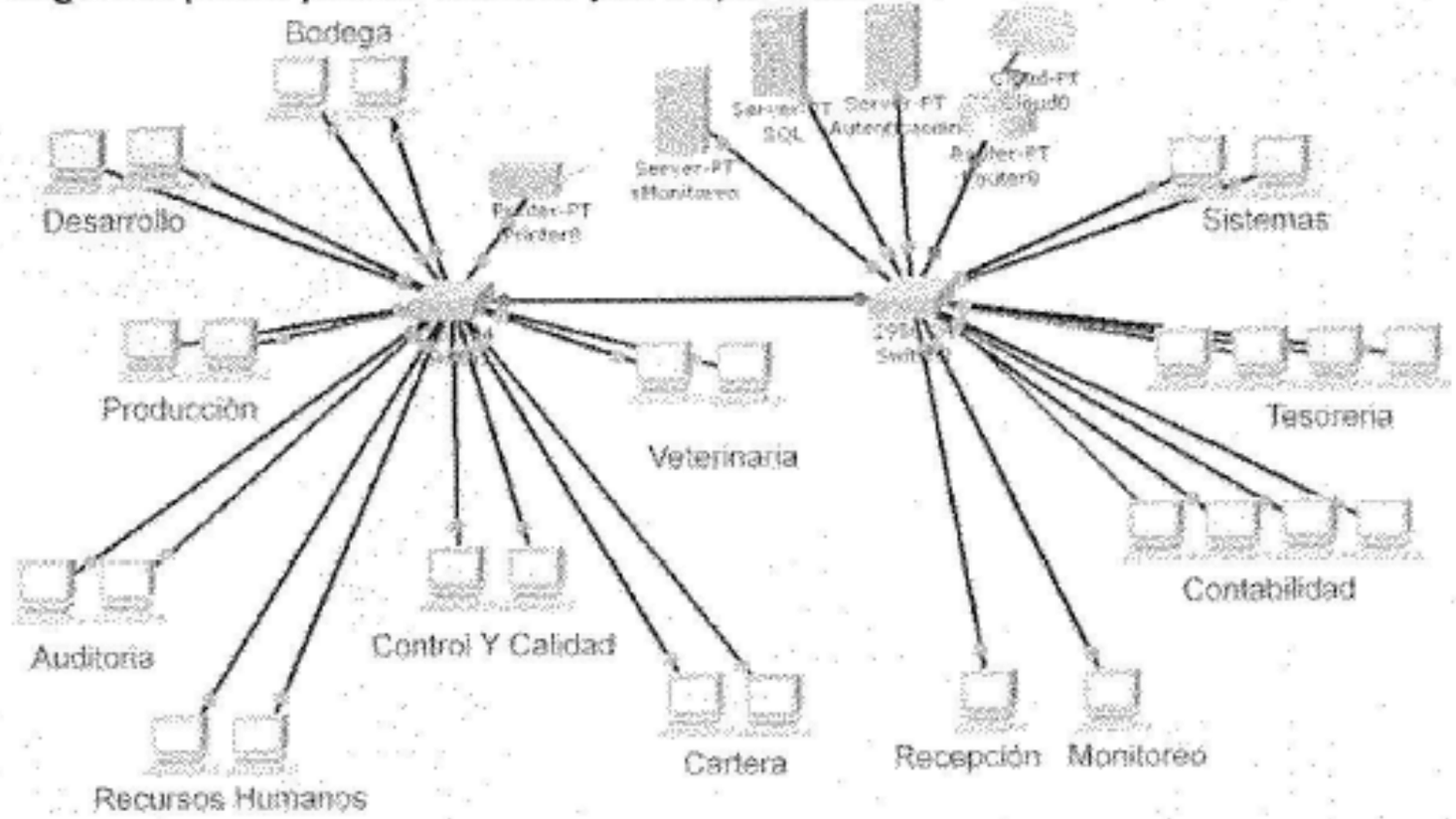


En el primer edificio contamos con 30 estaciones de trabajo que en total tiene 11 departamentos ubicados en el segundo piso que son sistema, contabilidad, tesorería, producción, desarrollo, auditoria, recursos humanos, control y calidad cartera veterinaria y Bodega.

En el primer piso del primer edificio hay 2 estaciones de trabajo, una encargada de de la recepción de la empresa y otra encargada del control y monitoreo de cámaras.

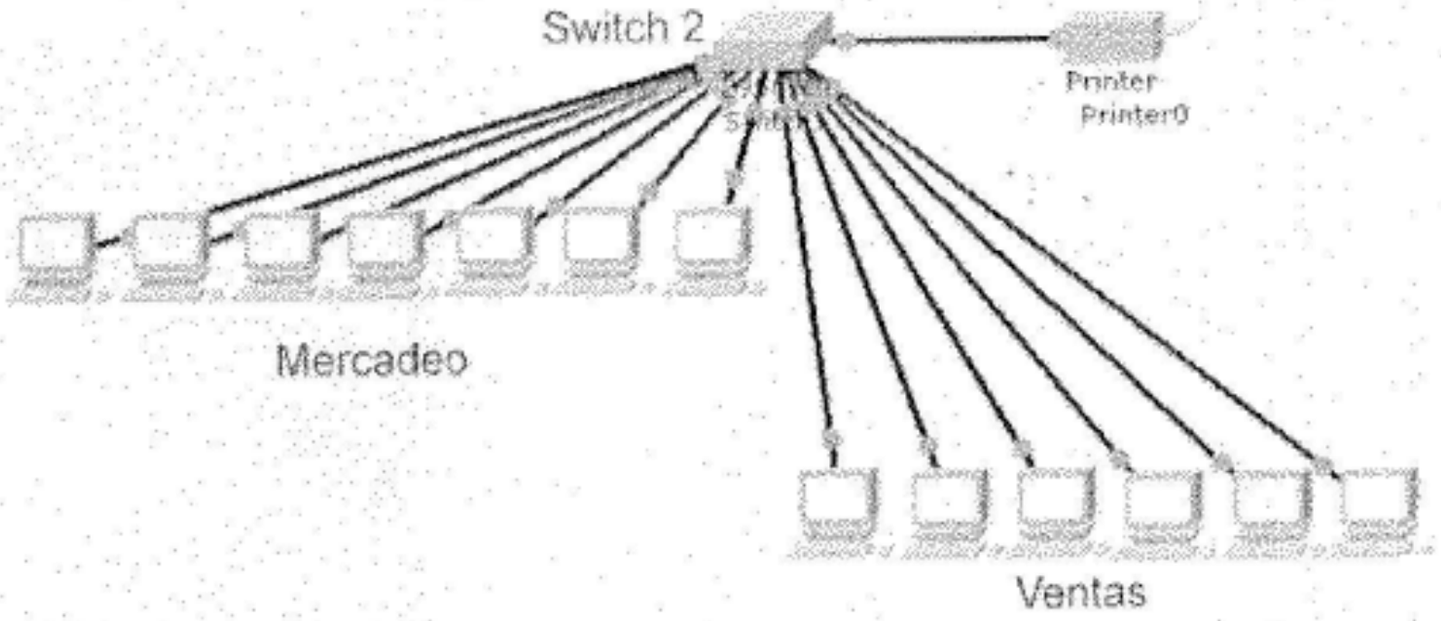


Segundo plano primer Edificio por Departamentos

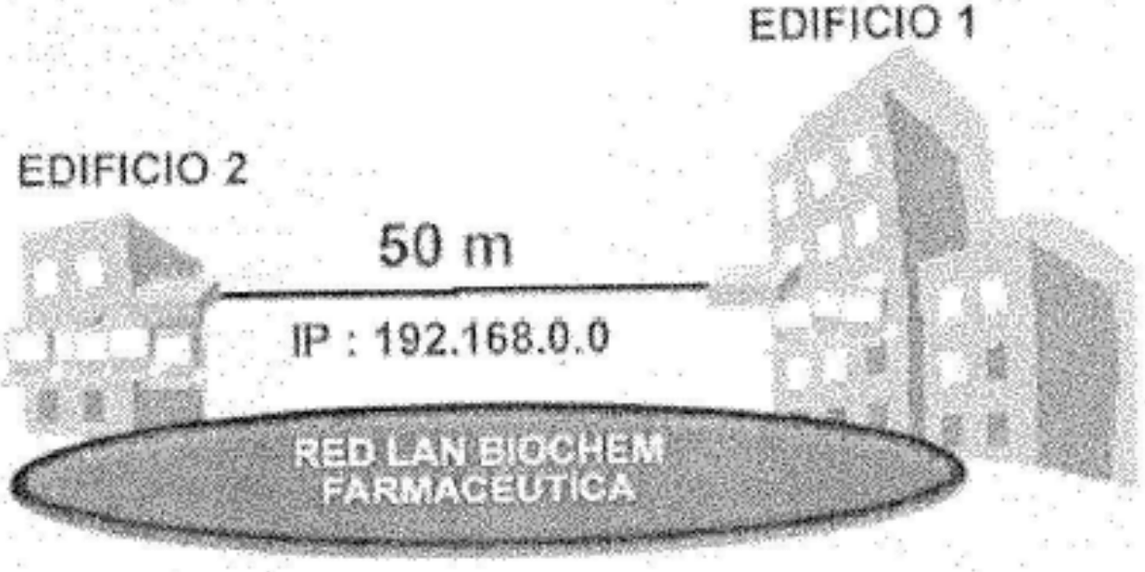


En el segundo edificio contamos con 13 estaciones de trabajo actualmente con dos departamentos que son los siguientes 6 estaciones de trabajo para Ventas y 7 Estaciones de Trabajo para mercadeo.

EDIFICIO DOS



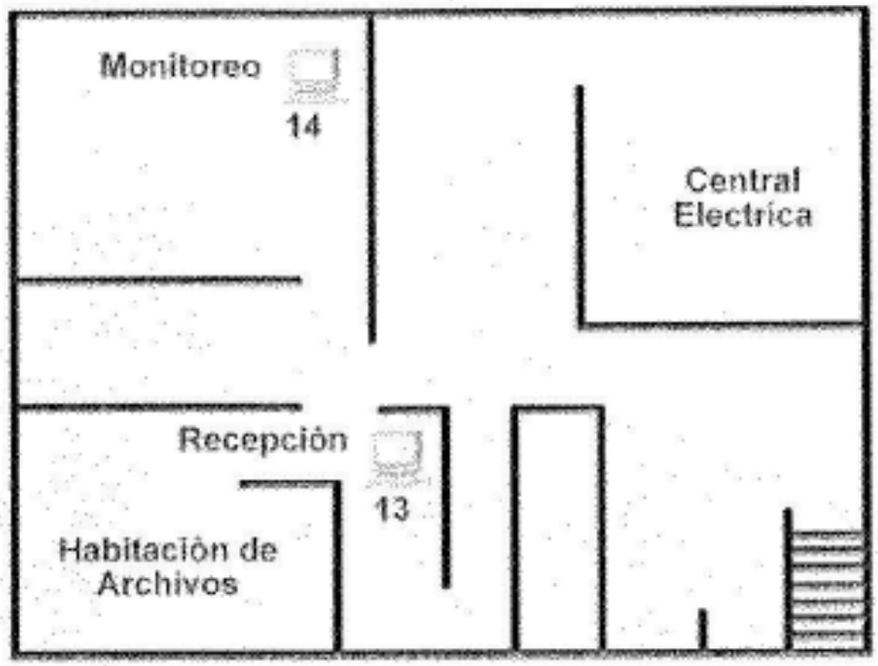
Aunque la red se encuentra separada en dos sedes o edificios , esto no implica que la red este segmentada en dos partes o más, en realidad es un conjunto, por lo que se dice que el rango de direcciones IP es el mismo en todos los departamentos y en las estaciones de trabajo, tal vez es mas fácil de administrar y mas fácil la interconexión entre equipos, pero esto implica mas trafico en la red debido a las peticiones ARP o Broadcast que solicita cada estación de trabajo.



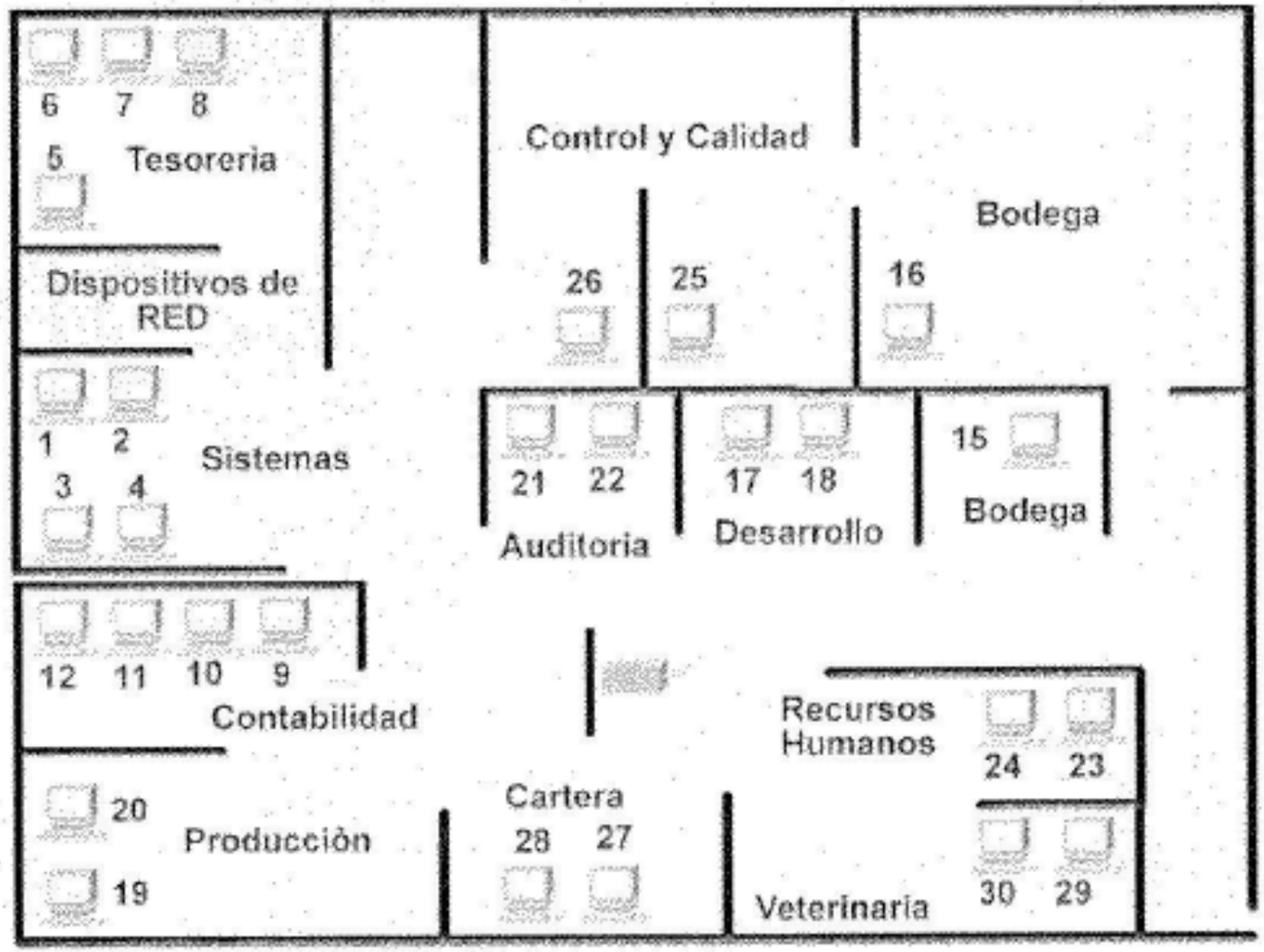
Distribución Lógica de Biochem Farmacéutica Actual es:

DEPARTAMENTO	EQUIPO	DIRECCION	SEDE	PISO
Sistemas	Host 1	192.168.0.3	Edificio 1	Piso 2
	Host 2	192.168.0.4	Edificio 1	Piso 2
	Host 3	192.168.0.5	Edificio 1	Piso 2
	Host 4	192.168.0.6	Edificio 1	Piso 2
Tesorería	Host 5	192.168.0.7	Edificio 1	Piso 2
	Host 6	192.168.0.8	Edificio 1	Piso 2
	Host 7	192.168.0.9	Edificio 1	Piso 2
	Host 8	192.168.0.10	Edificio 1	Piso 2
Contabilidad	Host 9	192.168.0.11	Edificio 1	Piso 2
	Host 10	192.168.0.12	Edificio 1	Piso 2
	Host 11	192.168.0.13	Edificio 1	Piso 2
	Host 12	192.168.0.14	Edificio 1	Piso 2
Recepción	Host 13	192.168.0.16	Edificio 1	Piso 1
Monitoreo	Host 14	192.168.0.17	Edificio 1	Piso 1
Bodega	Host 15	192.168.0.19	Edificio 1	Piso 2
	Host 16	192.168.0.20	Edificio 1	Piso 2
Desarrollo	Host 17	192.168.0.21	Edificio 1	Piso 2
	Host 18	192.168.0.22	Edificio 1	Piso 2
Producción	Host 19	192.168.0.23	Edificio 1	Piso 2
	Host 20	192.168.0.24	Edificio 1	Piso 2
Auditoria	Host 21	192.168.0.25	Edificio 1	Piso 2
	Host 22	192.168.0.26	Edificio 1	Piso 2
Recursos Humanos	Host 23	192.168.0.27	Edificio 1	Piso 2
	Host 24	192.168.0.28	Edificio 1	Piso 2
Control y Calidad	Host 25	192.168.0.31	Edificio 1	Piso 2
	Host 26	192.168.0.32	Edificio 1	Piso 2
Cartera	Host 27	192.168.0.33	Edificio 1	Piso 2
	Host 28	192.168.0.34	Edificio 1	Piso 2
Veterinaria	Host 29	192.168.0.35	Edificio 1	Piso 2
	Host 30	192.168.0.36	Edificio 1	Piso 2
Ventas	Host 31	192.168.0.41	Edificio 2	Piso 2
	Host 32	192.168.0.42	Edificio 2	Piso 2
	Host 33	192.168.0.43	Edificio 2	Piso 2
	Host 34	192.168.0.44	Edificio 2	Piso 2
	Host 35	192.168.0.45	Edificio 2	Piso 2
	Host 36	192.168.0.46	Edificio 2	Piso 2
Mercadeo	Host 37	192.168.0.47	Edificio 2	Piso 2
	Host 38	192.168.0.48	Edificio 2	Piso 2
	Host 39	192.168.0.49	Edificio 2	Piso 2
	Host 40	192.168.0.50	Edificio 2	Piso 2
	Host 41	192.168.0.51	Edificio 2	Piso 2
	Host 42	192.168.0.52	Edificio 2	Piso 2
	Host 43	192.168.0.53	Edificio 2	Piso 2

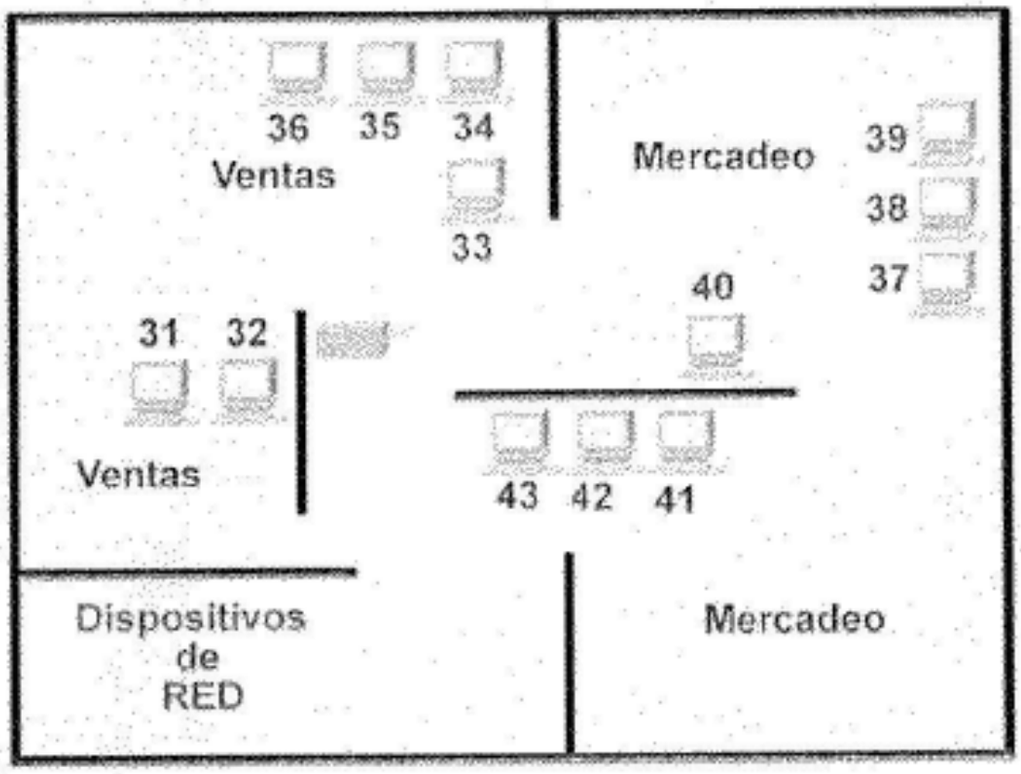
Distribución de las estaciones de Trabajo primer piso Edificio 1



Distribución de las estaciones de Trabajo Segundo piso Edificio 1



Distribución de las estaciones de Trabajo Segundo piso Edificio 2



3. DIAGNOSTICO DE LA RED

3.1 PRIMER PROBLEMA

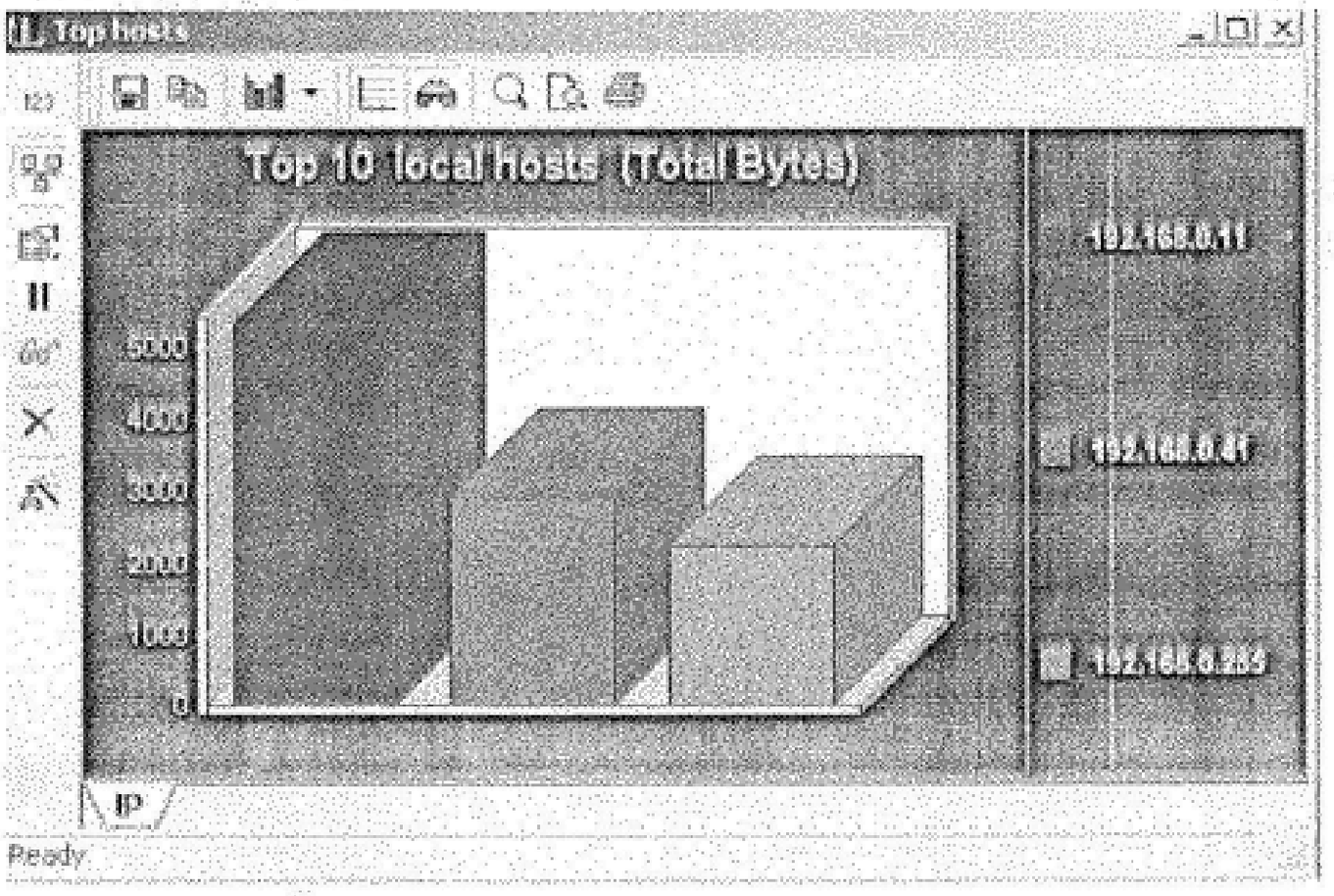
El problema actual de la compañía se evidencia en la perdida de velocidad de Internet y comunicación de la red LAN hacia la otra red que esta ubicada en el segundo edificio. Las causas pueden ser:

- Mal estado de los dispositivos
- Mucha difusión de broadcast en la segunda LAN
- Perdida de datos por el enlace UTP de 50 metros que establece la conexión de las dos sedes.

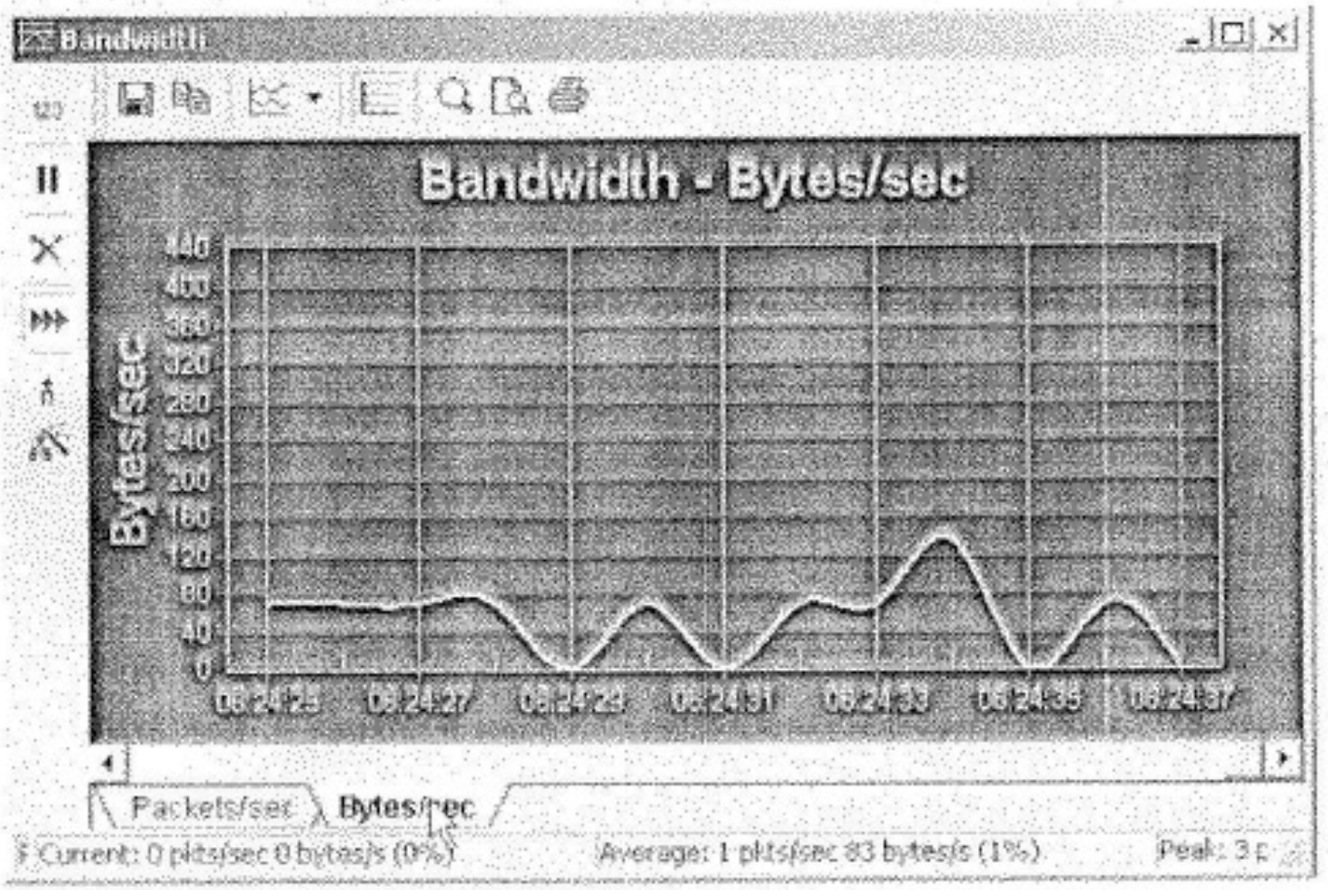
El primer paso analizar es el estado de los dispositivos que en este caso seria los swicth TRICOM superstar 3300XM pero estos por garantía y marca de por vida se excluyen. Sin embargo el trafico en la misma subred dos es estable y no hay demora ni perdida de información por transferencia de ficheros entre las estaciones de trabajo en los departamentos de venta y mercadeo. Por esto se descartaría y se concluirá que el swicth del segundo edificio esta en buen estado.

Después de realizar un intercambio de puertos, con el objetivo de detectar cualquier problema de funcionamiento en los puertos usados no se detecto ninguna irregularidad.

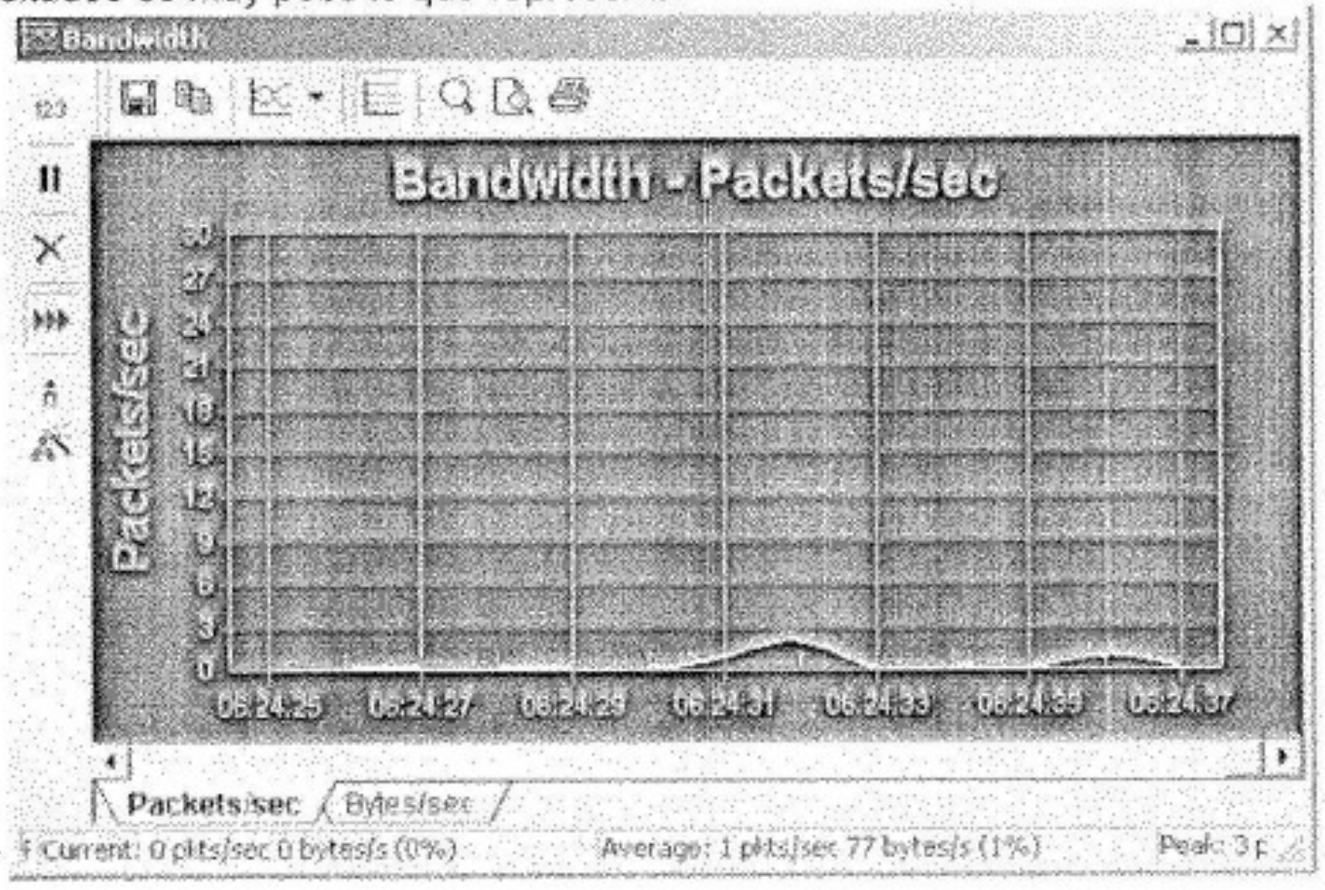
Con respecto a la hipótesis de difusión por broadcast o multicast se empezaría analizar si alguna estación de trabajo o todas ellas difunden muchas peticiones congestionado la red, este proceso se realizo verificándolo con un sniffer que se instalo en varias estaciones de trabajo y los resultados obtenidos fueron los siguientes:



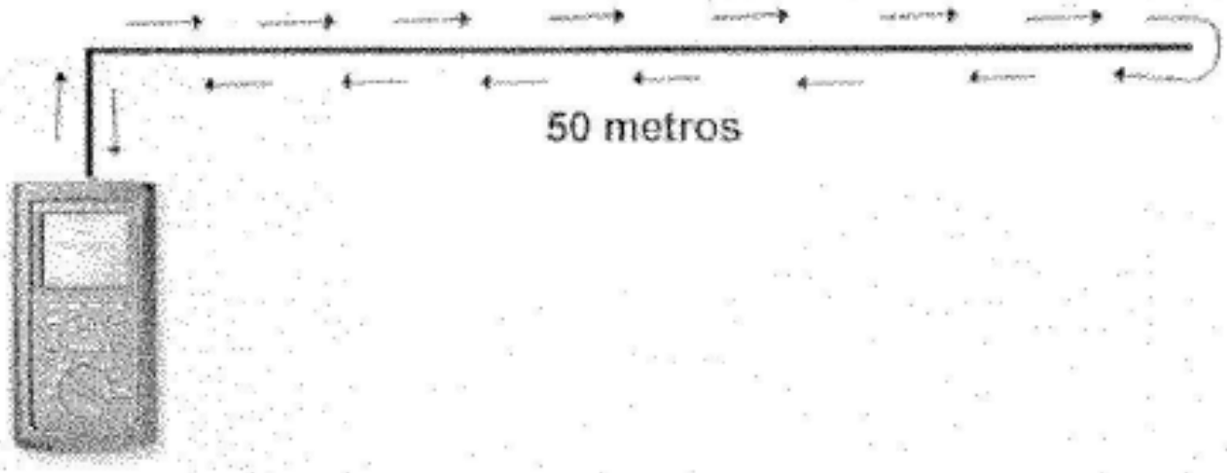
Como demuestra la grafica la estación de trabajo 192.168.0.11 que es el equipo numero 9 del departamento de contabilidad del primer edificio tiene un gran nivel de trafico con respecto al equipo numero 31 del departamento de ventas del segundo edificio, pero la cantidad comparada con respecto al trafico de broadcast que es 192.168.0.255 no representa problema sin embargo se analiza el ancho de banda del enlace que comunica las dos sedes y el resultado es el siguiente:



El ancho de banda tiene variaciones promedio de 120 bytes/sec por lo que es un promedio normal que no representa problema, aparte el promedio de Paquetes transitados es muy poco lo que representa.



Luego de descartar lo anterior además se realizaron pruebas de conectividad desde el primer edificio hacia el segundo con una herramienta que nos favoreció la empresa ya que es instrumento IEEE y TIA/EIA estándar establecido que permiten comprobar si la red está operando a un nivel aceptable. Este instrumento es un NetTool de Fluke.



Al realizar la prueba como resultado hubo una atenuación por el enlace UTP de 50m y una variación de ruido en la señal de transmisión eso quiere decir que este problema es debido al enlace de conexión entre las subredes de ambas sedes.

Para establecer la solución hay dos posibilidades:

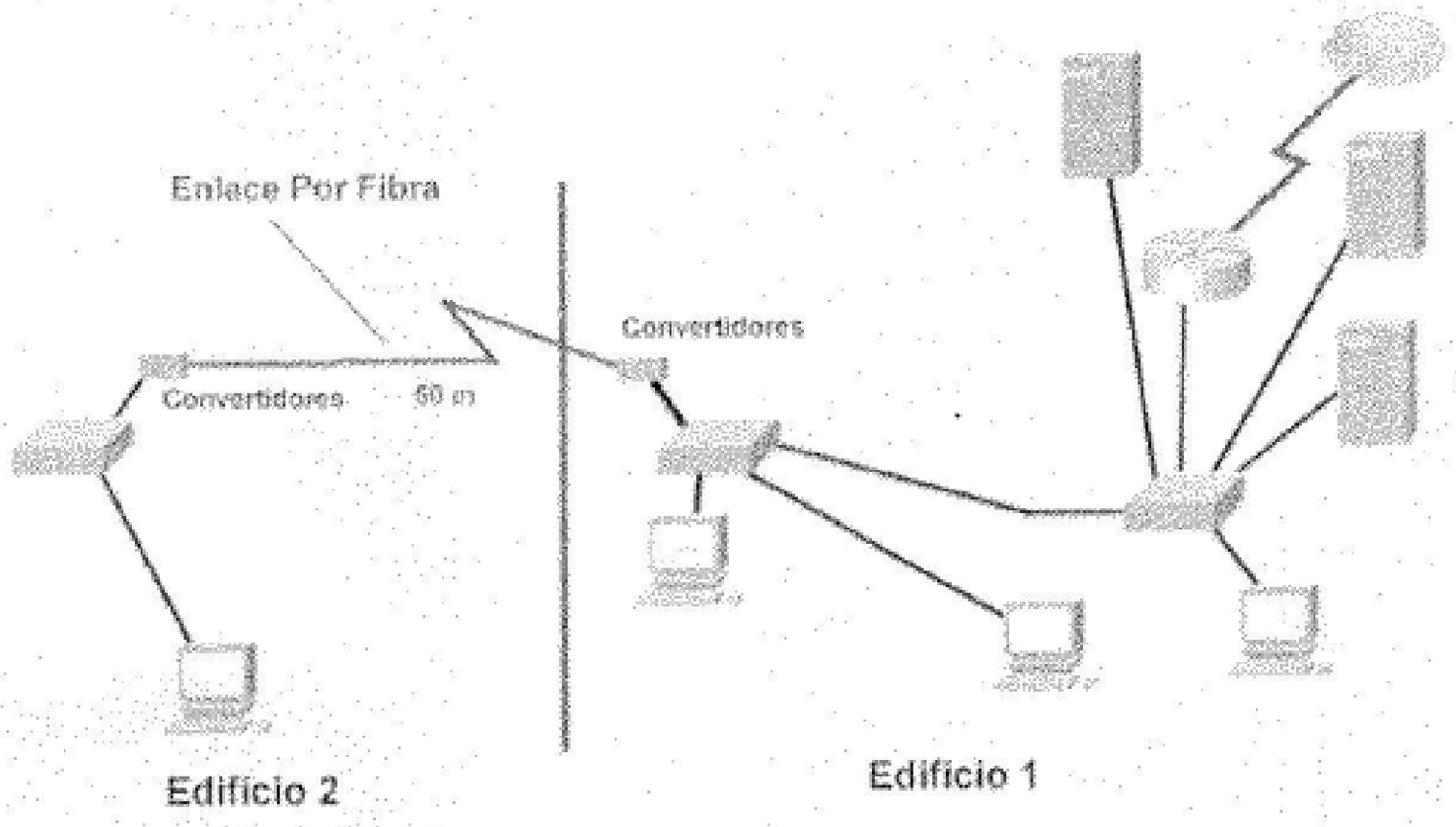
- Instalar un repetidor en el enlace
- Cambiar el enlace UTP por fibra óptica.

A pesar de que son 50m de distancia se empleo un categoría 5 E mejorada y este no presento cambios. La empresa a pesar de tener un buen cableado estructurado en cuanto a la parte eléctrica y de red cuentan también con una buena conexión a tierra, por el cual no hay interferencia de ruido eléctrico.

La instalación de un repetidor o hub es una solución mas viable con menor costo o presupuesto pero debido a una pequeña fabrica de tornillería y perforación de acero que esta ubicada cerca de BIOCHEM FARMACUTICA, esta perfilaría produce ruido eléctrico alrededor de la zona.

Resultados de de señal con ruido entre los enlaces:

Por esta causa y en mejorar el nivel de desempeño de la red a un futuro no muy lejano se ideo la implementación de conexión por fibra óptica multimodo.



Para implementar este medio de enlace se necesita aproximadamente 60 metros de fibra, también se necesitara dos dispositivos conversores de luz a datos como los transeivers una para cada edificio, debido a que los dispositivos como los swicth TRICOM superstar 3300XM que posee actualmente la empresa no tiene incorporado la conexión de fibra.

Los dispositivo Convertidores de fibra a implementar es:

Convertidor de fibra multimodo (tipo ST) de 10/100Base-TX a 100Base-FX

TFC-110MSTE

El Convertidor de medios de fibra serie TFC-110MSTE de TRENDnet transforma un medio UTP/STP 10/100Base-TX en un medio 100Base-FX y viceversa. El puerto 10/100Base-TX autonegocia velocidades de conexión de 10 ó 100Mbps con tipo de medios Auto-MDIX. La conexión de fibra puede ser de multimodo tipo ST. Este convertidor le ofrece a su Conmutador/Hub la capacidad de interconectarse a conexiones de fibra a una distancia de hasta 2 Km.

Características

- Compatible con los estándares IEEE 802.3 10Base-T y IEEE 802.3u 100Base-TX, 100Base-FX
- Ofrece autonegociación de un puerto 10/100Base-TX con conector RJ-45
- Ofrece fibra óptica multimodo con un puerto 100Base-FX con conector ST (TFC-110MSTE)
- Auto MDI-X para puerto 10/100Mbps-TX
- Autonegociación para modo de velocidad y de dúplex en puerto 10/100Mbps-TX
- Ofrece un interruptor deslizante para selección de Full y Half dúplex en puerto FX
- Conexión sin necesidad de apagar el equipo y para montaje en pared
- 5 años de garantía

Nombre del modelo	Longitud de onda	Medios	Salida de energía	Sensibilidad	Alimentación eléctrica
TFC-110MSCE	1310nm	MMF	-19dBm	-32dB	-21dB
TFC-110MSTE	1310nm	MMF	-19dBm	-32dB	-21dB

Especificaciones Técnicas

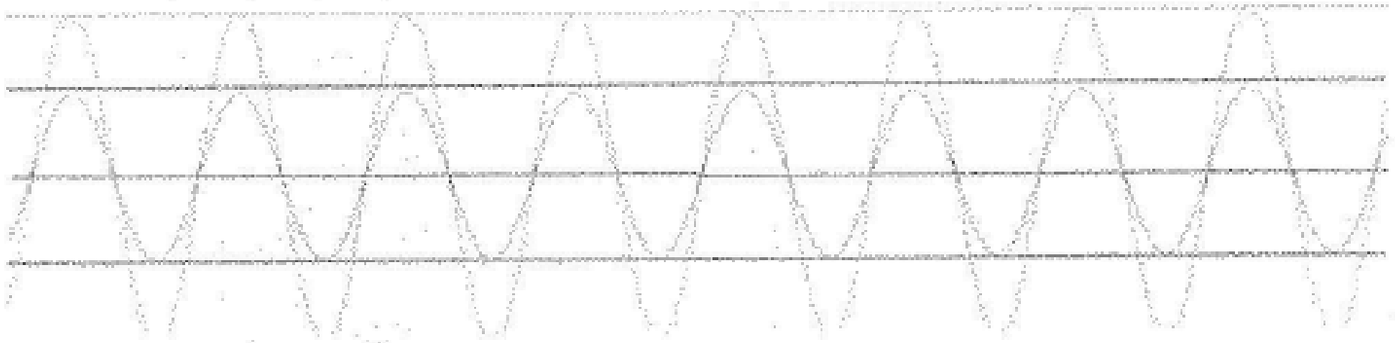
Hardware

Estándar:	• IEEE 802.3 10Base-T • IEEE 802.3u 100Base-TX y 100Base-FX
Medios de Red:	• 10Base-T: UTP Cat. 3, 4, 5, EIA/TIA-568 STP de 100 ohmios • 100Base-TX: UTP Cat. 5, EIA/TIA-568 STP de 100 ohmios • 100Base-FX: Cable de fibra óptica multimodo de 50/125 um ó 62.5/125 um, hasta 2 km
Protocolo:	CSMA/CD
Puertos:	• 1 x 10/100Base-TX

	• 1 x 100Base-FX
Velocidades de transferencia:	• 10Base-T: 10Mbps/20Mbps (Half/Full Dúplex) • 100Base-TX: 100Mbps/200Mbps (Half/Full Dúplex)
LEDs de diagnóstico:	• Por unidad: Alimentación eléctrica • Por puerto: Enlace/Actividad, Full Dúplex/Colisión
Adaptador de alimentación:	Adaptador eléctrico externo 1A y 7,5V DC
Consumo eléctrico:	2 vatios (máx.)
Dimensiones:	116 x 70 x 25mm (4,6 x 2,75 x 0,98 pulgadas)
Peso:	200g (7 onzas)
Temperatura:	• Operación: 0° ~ 40° C (32° ~ 104° F) • Almacenamiento: -25° ~ 70° C (-13° ~ 158° F)
Humedad:	5% ~ 90% RH
Certificación:	FCC, CE

la instalación y la implementación de los dispositivos convertidores de fibra se estima que el resultado en cuanto a las atenuaciones y variación de ruido electromagnético desaparezcan del enlace entre las dos sedes de la empresa. Al mismo tiempo se optimice el uso del ancho de banda ya que este medio favorece no solo ventajas de transmisión sino también de seguridad referente a la intercepción de datos por el mismo medio de fibra :

Resultado de señal por medio de fibra óptica:



3.2 SEGUNDO PROBLEMA

Otro de los problemas actuales en la empresa y en muchas otras también es el problema de la administración y control de servicios adicionales e innecesarios para las funciones laborales como por ejemplo:

- Messenger
- Chat
- Descarga de archivos multimedia
- Descarga de ficheros peligrosos

Este tipo de problema se podrá solucionar implementando servicios en los servidores existentes de autenticación, monitoreo y Base de Datos. Sin embargo los servidores de monitoreo y el de SQL necesitan toda la capacidad para su optimo desempeño por lo tanto se estudiara la posibilidad de implantar los servicios en el servidor de Autenticación de usuarios, pero este al igual que los otros necesita toda su capacidad y por normas políticas de seguridad de la empresa no admiten la adición de servicios a este servidor, ya que este no solo posee la autenticación de usuarios locales si no también usuarios de otras sedes a nivel nacional de BIOCHEM FARMACEUTICA.

Para solucionar este problema se necesitara implementar o adicionar otro servidor con los servicios mas necesarios y comunes como por ejemplo:

DHCP local
DNS local
Proxy
Firewall
Antivirus

Se implementa un Servidor HP ML370 con Windows 2003 Server, para instalar los servicios faltantes, además la falta de una pagina Web local y un dominio local hace necesario la adición de este Equipo.

El software a implementar como buen recurso para solucionar el problema de servicios que desvíen y decrementen las actividades laborales es el firewall:

3.2.1 ZoneAlarm

El programa es una barrera de protección frente a posibles ataques, muy rápido y que consume mucho menos recursos que otros Firewalls del mercado. controla la ejecución y autorización de los servicios de Internet tales como los protocolos de Correo POP3, SMTP, sitios web HTTP, IRC (Chat), Telnet, etc., mensajera instantánea (MSN Messenger, Netscape Messenger, Yahoo Messenger, ICQ, etc.), como los de redes de archivos compartidos Peer to Peer como KaZaa, eDonkey2000, Morpheus, etc.

Ventajas principales de ZoneAlarm Pro:

ZoneAlarm Pro le ofrece una eficaz seguridad en varios niveles, con un servidor de seguridad avanzado, aplicación anti-software espía, protección contra la suplantación de identidad, protección de la privacidad y otras funciones. Sus funciones, completas y fáciles de usar, pueden reforzar los programas antivirus o de servidor de seguridad básicos y son perfectas para todos los usuarios a quienes preocupe la privacidad en Internet.

Servidor de seguridad de la red y de los programas

Dotado de funciones preventivas de protección con varios niveles de seguridad, para detener los ataques entrantes, salientes y de los programas, de una forma completamente invisible para los piratas informáticos.

Protege el perímetro de la red de los ataques, tanto entrantes como salientes, con el servidor de seguridad Nº 1 del mundo.
Impide que el software espía y otros programas dañinos envíen sus datos personales a sitios de Internet.

Hace a su PC invisible para cualquier usuario de Internet.
Protege sus programas del código dañino.

Servidor de seguridad del sistema operativo OSFirewall

Este nivel adicional de seguridad impide la instalación en su PC del software espía, tan difícil de quitar posteriormente, y evita que pueda causar daños.

Supervisa la instalación de programas, los cambios en el Registro y el acceso a los archivos hasta en el núcleo de su PC.
Supervisa acciones adicionales de los programas para ampliar aún más la protección.

Evita que el software dañino llegue a dañar los archivos del núcleo del sistema operativo Windows.

Protección contra el robo de identidad

ZoneAlarm amplía la protección de los datos personales almacenados en su PC con nuevos servicios de protección contra el robo de identidad, que impiden, además del robo de la identidad a través de Internet, incluso el robo de la información en formato físico.

Anti-software espía

Funciona siempre al máximo rendimiento para detectar y eliminar el software espía antes de que se instale en su PC.

Mayor capacidad para eliminar incluso el software espía más tenaz y difícil de encontrar que haya podido infiltrarse hasta el núcleo de su PC.

Bloqueo de sitios espía

Impide que el software espía se infiltre en su PC, al bloquear su fuente principal: los sitios Web que distribuyen software espía.

Impide las visitas por accidente o por redirección a los sitios Web que distribuyen software espía.

Si el software espía ya se ha instalado en su equipo, le impide ponerse en contacto con otros sitios Web para intercambiar información, enviar sus datos personales o descargar actualizaciones.

Protección de la privacidad

Administra y bloquea los anuncios emergentes, el rastreo de sus hábitos en Internet, las cookies, la memoria caché y los archivos de comandos, para que pueda navegar sin ser molestado.

Modo de juegos

El control con un solo clic suspende provisionalmente la mayoría de las alertas de seguridad para que no interrumpan los juegos, sin rebajar por ello el nivel de protección máxima de su PC.

Seguridad indispensable del correo electrónico

Pone en cuarentena los archivos adjuntos recibidos por correo electrónico que parezcan sospechosos, para protegerle de los virus desconocidos; detiene automáticamente los mensajes enviados, para impedir que infecten accidentalmente a otros usuarios.

Protección de equipos inalámbricos

Detecta automáticamente las redes inalámbricas y protege su PC de piratas informáticos y otras amenazas de Internet, en su domicilio o mientras está de viaje.

Servicio SmartDefense

Proporciona a su PC actualizaciones de la seguridad en tiempo real, una respuesta mejorada al software espía que intente instalarse y nuevas funciones de protección contra ataques.

SmartDefense Advisor ajusta automáticamente los valores de seguridad para lograr la máxima protección contra las epidemias más recientes de virus y software espía.

Incluye DefenseNet, un sistema de alerta anticipada que obtiene información de la comunidad de usuarios de Zone Labs sobre los ataques más recientes de software espía y código dañino.

Rendimiento y compatibilidad superiores
Su PC se ejecutará siempre con rapidez y sin problemas.

Requisitos del sistema:

Windows 2000 Pro/XP. Pentium II a 450 MHz o superior. 50 MB de espacio libre en el disco duro. Acceso a Internet. RAM mínima del sistema: 64 MB (2000 Pro), 128 MB (XP). Más información

El software a implementar como buen recurso para solucionar el problema de control de acceso Web a sitios prohibidos con descarga de ficheros peligrosos que afecten a la red y a las estaciones de trabajo es el Proxy:

El software como buen recurso para el proxy es:

3.2.2 CProxy Anonymity 4 Server 3.4.3

Este Proxy permanece activo en la barra del sistema, sin ocupar espacio en tu escritorio, Este programa incluye una cache en la que se almacenará los sitios a los que mas frecuentemente acudamos en Internet. Soporta los protocolos HTTP, HTTPS, FTP, SOCKS, NNTP, SMTP, POP3 y Real Audio. También incluye soporte de mapeado tanto sobre UDP como TCP, para servicios personalizados, entre otras muchas e importantes opciones.

En todas las conexiones Web que hagas no aparecer la dirección que te suministra tu proveedor de Internet o la que tienes asignada en la empresa, sino otra: la del servidor proxy que hayas escogido.

Elige el que quieras a cada momento (incluso uno diferente por cada petición nueva), asigna cada ordenador de una red a un servidor proxy anónimo diferente, bloquea cookies, selecciona que información quieres que envié tu navegador, y mucho mas.

3.3 TERCER PROBLEMA

El problema actual de la compañía se evidencia en el exceso de tráfico de datos a través de la difusión de **broadcats** debido a que el diseño actual de la red en su parte lógica no cuenta con el desarrollo de redes VLANS.

La solución a este problema es básicamente la configuración de redes VLANS, por lo que implicara segmentar subredes por departamentos, pero los swicth que actualmente están implementados en la empresa no soportan etiquetado debido a la norma 802.1 Q , a base de lo anterior se necesitaran establecer 4 o mas conexiones de fibra óptica de edificio a edificio por lo cual seria algo abrumador y a aparte la capacidad de puertos del swiths se ocupan.

La necesidad de cambiar los swicth por otros de capa 3 que soporte la norma 802.1 Q seria la solución perfecta a este problema y al mismo tiempo actualizar la red y tener mejores dispositivos con un optimo desempeño..

El dispositivo de capa 3 a implementar es:

3.3.1 Switch Cisco Catalyst Express 500-24TT

DESCRIPCION	DESCRIPCION DETALLADA
Descripción	Catalyst Express 500-24TT Switch
Fabricante	Cisco
Arquitectura de Red Compatible	Ethernet - 100 Mbps Two-Pair (100BaseTX), Ethernet - 10Mbps Twisted Pair (10BaseT), Gigabit Ethernet - 1000 Mbps (1000BaseT)
Número de Puertos	24
Tipo de Switch	Switch LAN
Estándares	IEEE 802.1D, IEEE 802.1p, IEEE 802.1q, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3U-LAN, IEEE 802.3x, IEEE 802.3z
Peso	8 lbs.
Modo de comunicación	Full-Duplex, Half-Duplex
Velocidades de red	10 Mbps, 100 Mbps, 1000 Mbps
Tipo de conectores	Ethernet - RJ-45
Arquitectura de red	Ethernet - 100 Mbps Two-Pair (100BaseTX), Ethernet - 10Mbps Twisted Pair (10BaseT), Gigabit Ethernet - 1000 Mbps (1000BaseT)

Para interconectar y comunicar las redes VLAN entre si, adicionalmente se requiere un ROUTER que soporte la norma 802.1.Q.

El dispositivo acto a implementa es:

3.3.2 ROUTER Cisco 1811:

El router de servicios integrados Cisco 1800 Series entrega de manera inteligente servicios concurrentes altamente seguros, ofreciendo a los clientes de oficinas pequeñas un sistema único y resistente. Este router de alto desempeño toma ventaja de sus conexiones de banda ancha a la vez que entregan funciones claves para oficinas pequeñas como seguridad avanzada, administración remota y enlaces de soporte.

La arquitectura de la serie Cisco 1800 se ha diseñado para satisfacer los crecientes requisitos de las pequeñas y medianas empresas, para ofrecer servicios simultáneos y seguros.

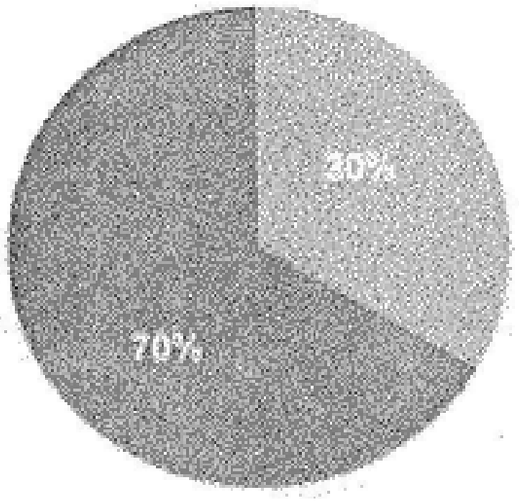
Descripción:

DESCRIPCION	DESCRIPCION DETALLADA
Descripción del producto	Cisco 1811 Integrated Services Router - encaminador
Tipo de dispositivo	Encaminador + conmutador de 8 puertos (integrado)
Factor de forma	Externo - 1U
Memoria RAM	128 MB (instalados) / 384 MB (máx.)
Memoria Flash	32 MB (instalados) / 128 MB (máx.)
Protocolo de direccionamiento	OSPF, RIP-1, RIP-2, BGP, EIGRP
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP, HTTP
Dimensiones	(Ancho x Profundidad x Altura) 34.3 cm x 27.4 cm x 4.4 cm Peso: 2.8 kg
Características	Cisco IOS Advanced IP services , protección firewall, cifrado del hardware, VPN, equilibrio de carga, soporte VLAN, Stateful Packet Inspection (SPI), activable, Sistema de prevención de intrusiones (IPS), filtrado de

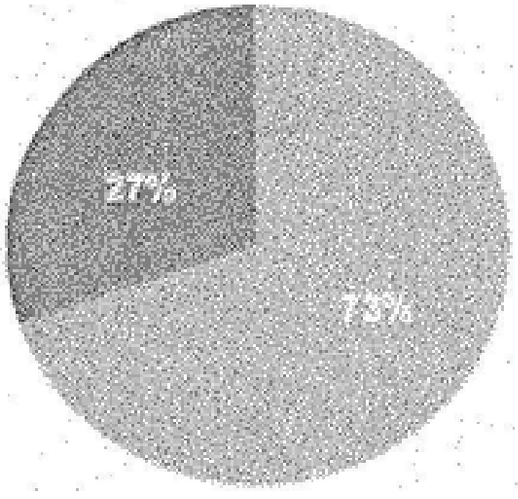
	URL
Cumplimiento de normas	IEEE 802.1Q
Alimentación	CA 120/230 V (50/60 Hz)

La implementación y segmentación por medio de redes virtuales como las VLANS y con la adecuación de nuevos dispositivos que soportan la norma IEEE 802.1Q implica tener mas ventaja con respecto al trafico de peticiones ARP o Broadcast, ya que adaptada esta solución el nivel de tráfico es mas optimo y recomendable para las funciones laborales actuales de la empresa, debido a que también se regula el ancho de banda.

3.3.3 Grafica Con respecto al tráfico



Trafico de RED Actualmente



Trafico de RED Con VLANS

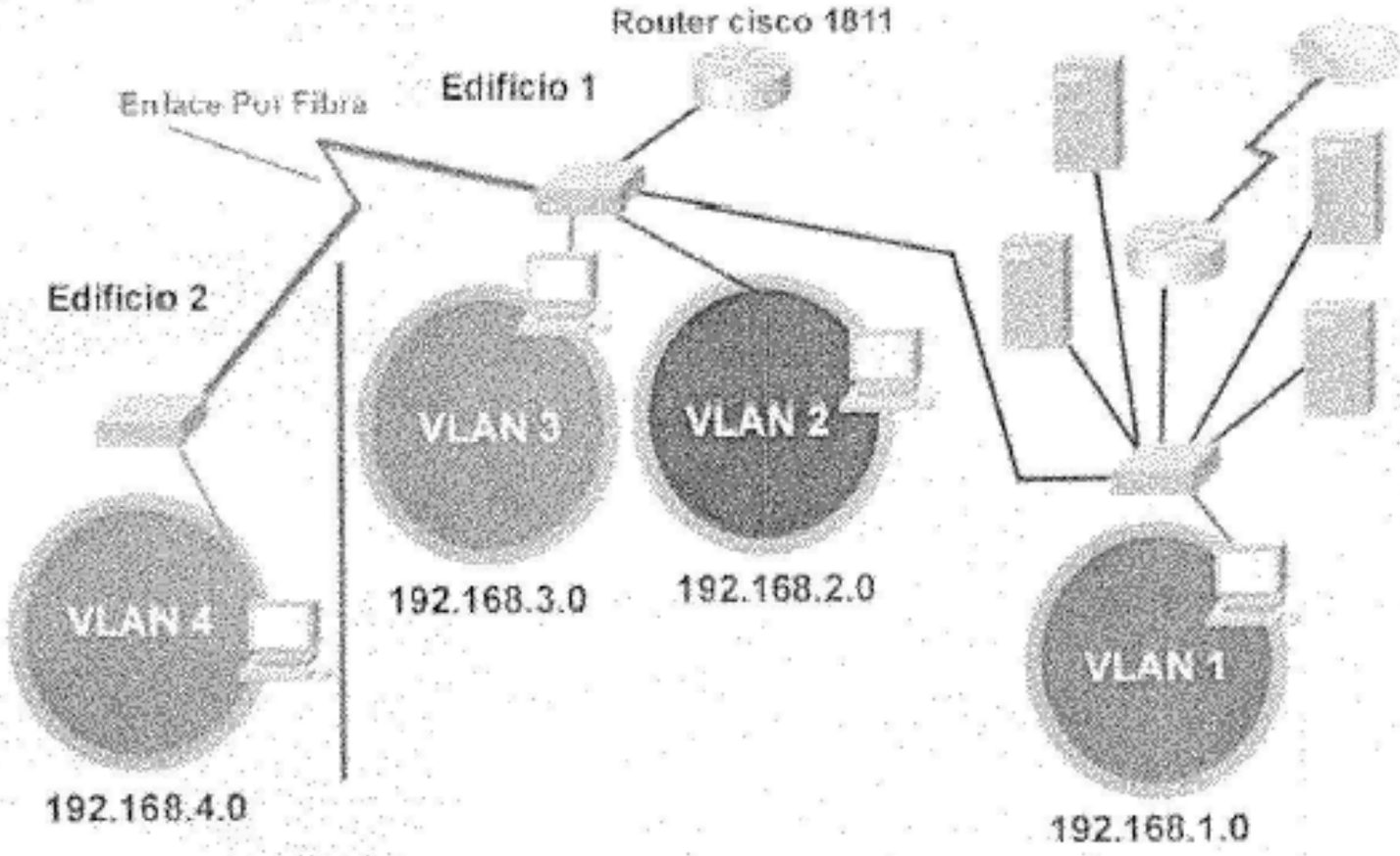
Petición ARP

Trafico TCP IP

Petición ARP

Trafico TCP IP

Red Con Implementación de VLANS



Distribución lógica a asignar:

DEPARTAMENTO	EQUIPO	DIRECCION	SEDE	VLAN
Sistemas	Host 1	192.168.1.3	Edificio 1	VALN 1
	Host 2	192.168.1.4	Edificio 1	VALN 1
	Host 3	192.168.1.5	Edificio 1	VALN 1
	Host 4	192.168.1.6	Edificio 1	VALN 1
Tesorería	Host 5	192.168.1.7	Edificio 1	VALN 1
	Host 6	192.168.1.8	Edificio 1	VALN 1
	Host 7	192.168.1.9	Edificio 1	VALN 1
	Host 8	192.168.1.10	Edificio 1	VALN 1
Contabilidad	Host 9	192.168.1.11	Edificio 1	VALN 1
	Host 10	192.168.1.12	Edificio 1	VALN 1
	Host 11	192.168.1.13	Edificio 1	VALN 1
	Host 12	192.168.1.14	Edificio 1	VALN 1
Recepción	Host 13	192.168.1.16	Edificio 1	VALN 1
Monitoreo	Host 14	192.168.1.17	Edificio 1	VALN 1
Bodega	Host 15	192.168.2.2	Edificio 1	VLAN 2
	Host 16	192.168.2.3	Edificio 1	VLAN 2
Desarrollo	Host 17	192.168.2.4	Edificio 1	VLAN 2
	Host 18	192.168.2.5	Edificio 1	VLAN 2

Producción	Host 19	192.168.2.6	Edificio 1	VLAN 2
	Host 20	192.168.2.7	Edificio 1	VLAN 2
Auditoria	Host 21	192.168.2.8	Edificio 1	VLAN 2
	Host 22	192.168.2.9	Edificio 1	VLAN 2
Recursos Humanos	Host 23	192.168.3.1	Edificio 1	VLAN 3
	Host 24	192.168.3.2	Edificio 1	VLAN 3
Control y Calidad	Host 25	192.168.3.3	Edificio 1	VLAN 3
	Host 26	192.168.3.4	Edificio 1	VLAN 3
Cartera	Host 27	192.168.3.5	Edificio 1	VLAN 3
	Host 28	192.168.3.6	Edificio 1	VLAN 3
Veterinaria	Host 29	192.168.3.7	Edificio 1	VLAN 3
	Host 30	192.168.3.8	Edificio 1	VLAN 3
Ventas	Host 31	192.168.4.4	Edificio 2	VLAN 4
	Host 32	192.168.4.5	Edificio 2	VLAN 4
	Host 33	192.168.4.6	Edificio 2	VLAN 4
	Host 34	192.168.4.7	Edificio 2	VLAN 4
	Host 35	192.168.4.8	Edificio 2	VLAN 4
	Host 36	192.168.4.9	Edificio 2	VLAN 4
Mercadeo	Host 37	192.168.4.10	Edificio 2	VLAN 4
	Host 38	192.168.4.11	Edificio 2	VLAN 4
	Host 39	192.168.4.12	Edificio 2	VLAN 4
	Host 40	192.168.4.13	Edificio 2	VLAN 4
	Host 41	192.168.4.14	Edificio 2	VLAN 4
	Host 42	192.168.4.15	Edificio 2	VLAN 4
	Host 43	192.168.4.16	Edificio 2	VLAN 4

4. COSTO DEL PROYECTO

Costo enlace de fibra óptica			
Cantidad	Articulo	Precio unitario	Precio total
60	Metro de fibra óptica multimodo 62.5/125 3mm Riser	$2.600	$156.000
4	Conectores ST Duplex Multimodo AMP 3mm	$6.900	$27.600
1	Trendnet - Conversor de 10/100BaseTx a 100BaseFX Multi Modo, ST	$295.900	$295.900
	Total	**$305.400**	**$479.500**

Costo servidor Windows y servicios			
Cantidad	Articulo	Precio unitario	Precio total
1	HP ML370	$3`757.600	$3`757.600
1	Licencia Server 2003	$1`156.000	$1`156.000
1	ZoneAlarm	$150.000	$150.000
1	CProxy Anonymity 4 Server	$85.000	$85.000
5	Conectores RJ45	$500	$2500
2	Metro UTP CAT 5E	$800	$1600
	Total	**$5`149.900**	**$5`152.700**

Costo implementación VLANS			
Cantidad	Articulo	Precio unitario	Precio total
3	Swicth cisco catalyst Express 500-24tt	$1`550.000	$4`650.000
1	Router cisco 1811	$2`600000	$2`600000
4	Conectores RJ45	$500	$2000
3	Metro UTP CAT 5E	$800	$2400
	Total	**$4`151.300**	**$7`254.400**

COSTO PROYECTO TOTAL	
Costo enlace de fibra óptica	$479.500
Costo servidor Windows y servicios	$5`152.700
Costo implementación VLANS	$7`254.400
Total	**$12`886.600**

RECOMENDACIONES

- Se recomienda la instalación de un enlace por fibra óptica multimodo cuando hay zonas con fábricas y talleres que por su actividad comercial dependan de un alto consumo eléctrico. Ya que por medio de este consumo se genera mucha interferencia electromagnética.

- Se recomienda la instalación de firewall y proxy para poder controlar las comunicaciones internas y externas de la empresa y además garantizar seguridad informática contra intrusos.

- Se recomienda la actualización y soluciones en cuanto a segmentación de subredes, para disminuir tráfico y control de broadcast y al mismo tiempo tener dispositivos que garantizan un óptimo rendimiento y seguridad al mismo tiempo.

CONCLUSIONES

- Los medios de conexión por cobre es una solución menos costosa pero genera más perdidas si no esta en condiciones óptimas y aceptables.

- La implementación de un enlace por fibra óptica a pesar de ser un poco más costoso, garantiza un óptimo desempeño en la trasmisión debido a su gran velocidad y al mismo tiempo aisla interferencias electromagnéticas que puedan generar ruido.

- La solución por fibra óptica también garantiza la seguridad de información en cuanto a trasmisión y a intercepción de intrusos.

- La implementación de servicios de seguridad como el proxy y el firewall son necesarios en todo tipo de empresa laboral.

- Las redes segmentadas por redes virtuales como las VLANS, mejoran el control de peticiones ARP o broadcast, y al mismo tiempo el nivel laboral.

BIBLIOGRAFÍA

WIKIPEDIA, Marca Registrada de Wikimedia Foundation, Inc (2006). http://es.wikipedia.org

LUCAS Morea / Sinexi S.A Monografías, (1997). http://www.monografias.com

CUERVO, F., GREENE, N., HUITEMA, C., RAYHAN, A., ROSEN, B. y SEGERS, J. (2000).

MEGACO, Protocol versión 0.8. RFC 2885, Agosto 2000.

GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol
Architecture and Requeriments. RFC 2805, Abril 2000.