CORPORACIÓN UNIVERSITARIA
UNITEC
CICLO PREPRATORIO DE GRADO
(CPG)

UNILAN

DAYANA EMILIA FORERO
DIANA CRISTINA HERRERA
JAVIER PEDRAZA GOMEZ
CARLOS ANDRES SOCHA

PROFESOR:
OSCAR TORRES

BOGOTÁ DC.
DICIEMBRE DE 2006

TABLA DE CONTENIDO

INTRODUCCIÓN

La situación tecnológica que se vive en este momento en nuestra sociedad y en nuestra vida cotidiana, nos hace partícipes de los cambios que en ella incurren para tener un mejor modo de vida.

Necesidades como la accesibilidad a las diferentes formas de comunicarse entre empresas, ha generado que estas, estén siempre cambiando y actualizando sus modos y formas para comunicarse rápida y eficazmente.

Queremos ser facilitadores para solucionarlas, aplicando conocimientos adquiridos en nuestra carrera y esperamos que este proyecto genere un crecimiento a nivel económico un mayor desarrollo a la empresa.

1. OBJETIVO GENERAL

Presentar una propuesta de solución de Red que incluya los esquemas físicos y lógicos de la red LAN, perteneciente a la empresa Metaliza Ltda.

2. OBJETIVOS ESPECÍFICOS

1. Identificar las necesidades de la empresa a nivel de comunicación.
2. Conocer las falencias físicas que se puedan presentar en la ampliación de las redes.
3. Verificar los servicios que sean realmente necesarios para la empresa, en especial dependiendo del Tipo de Aplicaciones.
4. Elaborar la documentación de la red propuesta.
5. Proponer politicas de seguridad en la red.
6. Presentar varias alternativas para la consideración de la gerencia de la Empresa

3. MARCO TEORICO

Las Redes de datos se desarrollaron como consecuencia de que las empresas necesitaban intercambiar información electrónica a grandes distancias; las empresas necesitaban una solución que resolviera los siguientes problemas:

- Evitar la duplicidad de equipamiento y recursos
- Comunicarse de forma eficaz
- Configurar y administrar una red.

Se crearon diferentes tipos de redes las cuales son:

1. Redes de Área Local (LAN):

Permiten a las empresas que empleen tecnología de computación compartir local y eficazmente ficheros e impresoras, y posibilitar las comunicaciones internas, como el correo electrónico. Las redes Lan están diseñadas para hacer lo siguiente:

- Operar dentro de una zona geográfica limitada.
- Permitir a muchos usuarios acceder a medios de gran ancho de banda.
- Proporcionar conectividad a tiempo completo a los servicios locales.
- Conectar físicamente dispositivos adyacentes.

Algunas tecnologías LAN comunes son:

- Ethernet
- Token Ring
- FDDI

2. Redes de Área Amplia (WAN):

Interconectan LAN que proporcionan acceso a computadoras o servidores de ficheros en otros lugares. Las WAN conectan redes de usuario sobre un área geográfica grande, esta hace posible que las empresas puedan comunicarse a grandes distancias. Las redes WAN están diseñadas para hacer lo siguiente:

- Operar sobre grandes áreas geográficamente separadas.
- Permitir que los usuarios mantengan una comunicación en tiempo real con otros usuarios.
- Proporcionar recursos remotos a tiempo completo conectados a los servicios locales.
- Ofrecer servicios de correo electrónico, WWW, transferencia de ficheros y comercio electrónico.

Algunas tecnologías WAN comunes:

- Modems
- RDSI (Red Digital de Servicios Integrados)
- DSL (Línea de Abonado Digital)
- Frame Relay
- Series de Portadoras T y E
- Red óptica sincronia.

3. Redes de Área Metropolitana (MAN):

Es una red que se extiende por un área metropolitana, como una ciudad o un área suburbana. Las MAN son redes que conectan LAN separadas por la distancia y que están ubicadas dentro de un área geográfica común.

4. PLANTEAMIENTO DEL PROBLEMA

¿Es necesario realizar el montaje de la red LAN en la empresa?

El avance tecnológico obliga a las empresas a realizar actualizaciones y ampliaciones de las redes físicas - lógicas para poder tener intercomunicación con el mundo interior y exterior.

Este proceso requiere de inversiones en hardware y software necesarios para la interconexión de los distintos dispositivos y el tratamiento de la información.

En una empresa suelen existir muchos ordenadores, los cuales requieren de muchos servicios y la solución para que no se vea afectada la eficiencia de las máquinas es la instalación de la red LAN.

En la empresa actualmente existen doce equipos de computo instalados en las áreas administrativa, de compras, de contabilidad y producción; los cuales aunque son de la misma empresa no pueden intercambiar toda la información que necesitan ya que se encuentran conectados únicamente ocho equipos por medio de un switch el cual solo se encarga de conmutar los paquetes ya que no es administrable; los cuatro PC restantes están sin conexión a la red existente.

5. JUSTIFICACIÓN

El proyecto es de gran importancia para la Empresa ya que le permitirá tener un mejor desarrollo a nivel interno, externo y de estructura fisica.
Toda vez que los usuarios quieran acceder, no solo en las áreas que desempeñan labores, si no que también lo podrán hacer en sitios donde antes no se podia confirmar ninguna información.

Además es de gran importancia por el nivel de desarrollo de las comunicaciones, ya que las empresas deben pensar cada día en surgir, actualizarse y en especial la tecnologia.

Adicionalmente, la empresa aportará todos los recursos necesarios para poder llevar a cabo esta labor.

6. METALIZA LTDA

Es una empresa que ofrece los siguientes servicios:

1. Sistema de electrometalizado selectivo y en frio.
2. Aplicaciones en metalización selectiva en frío.
3. Servicios de mecanizados.
4. Servicios de todo tipo de soldaduras calificadas.

METALIZA LTDA

ORGANIGRAMA DE LA EMPRESA

8. FACTIBILIDAD

Económica: La empresa dispone de un capital no despreciable para realizar la compra de la infraestructura de conexión y equipos que hagan falta para poner a funcionar la red LAN y consideran la implementación de la Red como una prioridad para su empresa.

Técnica: Adquisición de equipos, adecuación centro de computo (Rack, Servidores, Concentradores, Switch y Enrutadores), Canaletas, Cables, adecuación de puntos para conexión a Datos y Telefonia.

Operativa: Plan de visitas, toma de requerimientos, diseño de red, montaje de red, pruebas y entrega, los cuales están previstos para el desarrollo del proyecto.

9. MÉTODOS DE RECOLECCIÓN DE INFORMACIÓN

Se recogerá la información por medio de encuestas que se harán entre los empleados, ya que ellos nos darán a saber cuales son las verdaderas carencias, de información y necesidades que tiene la empresa.

ENCUESTA:

Nombre: _____

Fecha: _____

Departamento: _____

Cargo: _____

1. Cuales son lo problemas mas frecuentes con la comunicación entre departamentos?

_____

_____

2. Por que cree usted que suceden dichos problemas?

_____

_____

_____

3. Como cree usted que podría darse solución a dichos problemas con la intercomunicación?

_____

_____

4. Usted cree necesario implementar una red Lan en su empresa?

Si _____

No _____

5. Que tipos de documentos e información manejan a diario en la empresa?

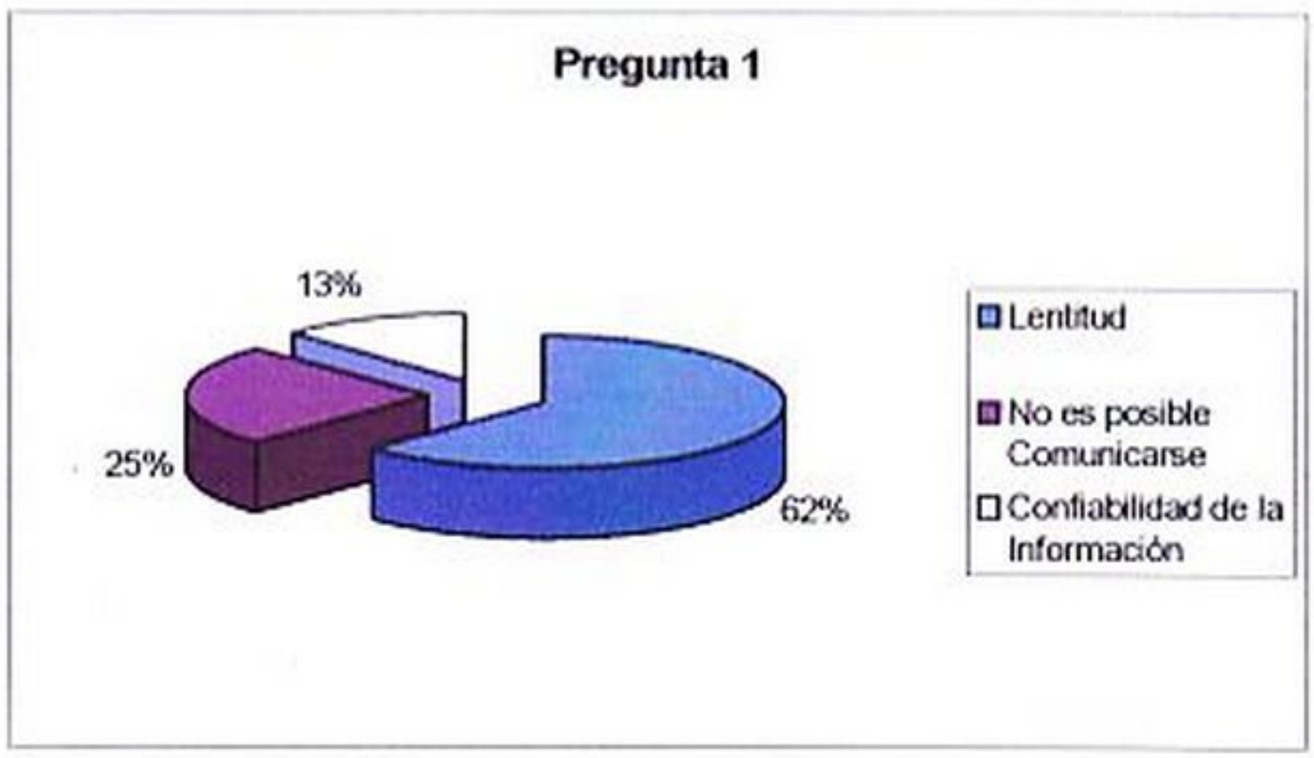
_____

_____

9.1 Se realizaron 40 encuestas y arrojaron los siguientes resultados:

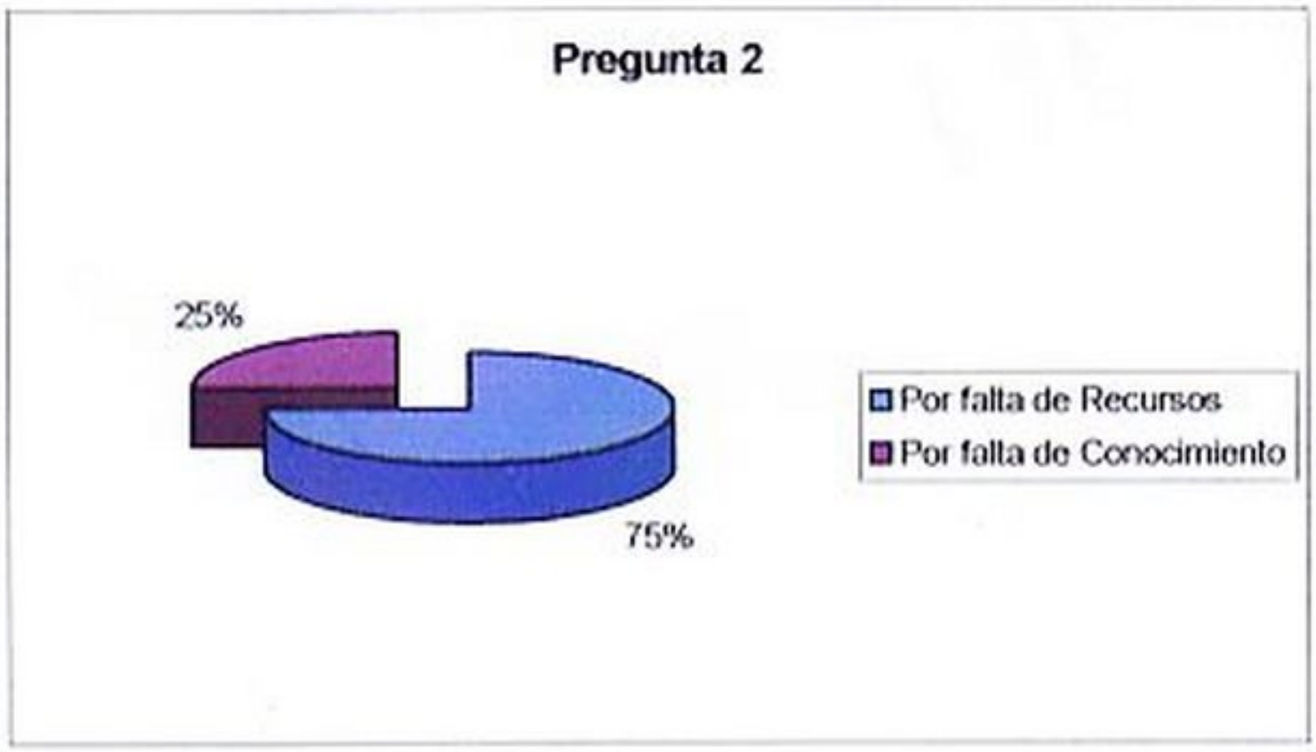
- **Pregunta 1:**

Respuestas	Resultados
Lentitud	25
No es posible Comunicarse	10
Confiabilidad de la Información	5



- **Pregunta 2:**

Respuestas	Resultados
Por falta de Recursos	30
Por falta de Conocimiento	10

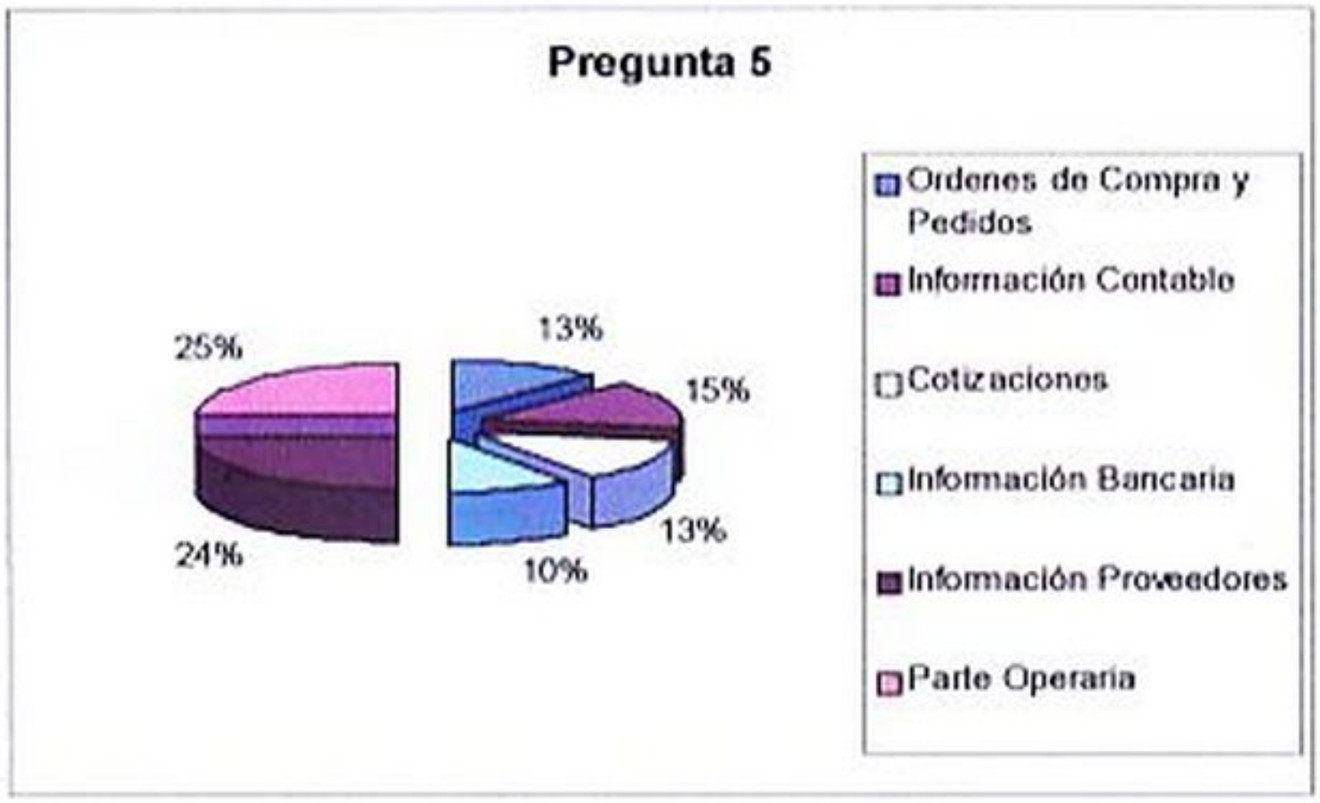


- **Pregunta 3:**

Respuestas	Resultados
Interconectando la Red	26
Contratando un Ingeniero de Sistemas	5
Adquiriendo equipos nuevos	5
No sabe/No responde	4

- **Pregunta 5:**

Respuestas	Resultados
Ordenes de Compra y Pedidos	5
Información Contable	6
Cotizaciones	5
Información Bancaria	4
Información Proveedores	10
Parte Operaria	10



10. CAPA FÍSICA

Esta capa se basa en el protocolo Ethernet IEEE 802.3, el cual hace referencia a las LAN de acceso múltiple con Detección de Portadora y Detección de Colisiones CSMA/CD, que transportan datos a altas velocidades en distancias limitadas, este protocolo especifica una red de topologia en Bus con un cable que conecta las estaciones finales y el medio de la red real.

Funciona a 10 Mb sobre cable coaxial o de par trenzado; gracias a su flexibilidad, su fácil implementación y entendimiento se conoce como tecnologia de medios.

Las especificaciones para el cable y el conector que se emplean para soportar las implementaciones Ethernet se derivan de las normas de cableado de telecomunicaciones (EIA/TIA-568) que especifica un conector RJ45 para un cable UTP.

En las redes actuales se debe utilizar un cable UTP Cat5 para soportar las conexiones de 10 a 1000 Mb.

Para interconectar diferentes dispositivos de las redes debemos emplear cables cruzados o directos dependiendo el tipo:

- **Cable Directo:** conexión de Switch a Router; de Switch a PC o Servidor y de Hub a PC o Servidor.
- **Cable Cruzado:** conexión de Switch a Switch; de Switch a Hub; de Hub a Hub; de Router a Router; de PC a PC y de Router a PC.

Para crear una red se emplean diferentes dispositivos llamados componentes de Hardware de la red:

- **REPETIDORES:** Estos dispositivos se utilizan para regenerar y resincronizar las señales de la red a nivel de los bits para permitirlas

viajar a largas distancias a través del medio. Se utilizan normalmente si existen muchos nodos de red o si el número de cables es insuficiente.

- **HUBS:** Son repetidores multipuerto, un HUB tiene entre 4 a 24 puertos, estos son implementados con mas frecuencia en redes Ethernet 10Base-T o 100Base-T, el uso del Hub cambia la topología de la red de un bus lineal, donde cada dispositivo se conecta directamente al hilo (Topología de Estrella), cuando todos los datos llegan a través de los cables a un puerto Hub, se repiten eléctricamente en todos los puertos conectados al mismo segmento de la red excepto al puerto del que se enviaron. Todos los dispositivos conectados a un Hub escuchan todo el tráfico, por tanto los Hubs mantienen un sencillo dominio de colisión.

Para la comunicación de los dispositivos de la red es necesario que exista cable para conectarlos, los tipos de cable utilizados para las telecomunicaciones son en medios de cobre, que son los mas comunes para el cableado de señal; los hilos de cobre son los componentes de un cable que transporta la señales desde un Host origen a un Host destino, el cobre tiene algunas propiedades importantes que lo hacen muy adecuado para el cableado electrónico:

- **Conductividad:** Es el mejor conductor de corriente eléctrica que se conoce
- **Resistencia a la Corrosión:** El cobre no se oxida y es bastante resistente a la corrosión.
- **Ductilidad:** Posee la capacidad de dividirse en finos hilos sin romperse.
- **Maleabilidad:** El cobre es muy maleable, ósea fácil de dar forma.
- **Fuerza:** El cobre mantiene la fuerza y dureza hasta cerca de los 204° C.

Hay dos tipos de Cable de Cobre utilizado para las redes:

COAXIAL: Este cable tiene un conductor central compuesto por un hilo de cobre sólido o un manojo de hilos, sirve para conexiones de Redes LAN y principalmente se emplea en conexiones de video, conexiones de alta velocidad como las líneas T3 ó E3 y la televisión por cable.
Esta constituido de un Conductor de cobre, u aislante plástico, una pantalla de cobre trenzada y una cubierta exterior. Este cable tiene su propio conector es el BNC (Conector Naval Británico), en el pasado este tipo de cable era el mas popular para las redes LAN ya que cubría mas distancias con menos repetidores entre nodos de la red, aunque por supuesto era mucho mas costoso que el cable STP ó UTP. Una gran desventaja de este cable es que el conductor exterior debe estar cuidadosamente y adecuadamente conectado a tierra, lo que incrementa la complejidad de la instalación, por esto ya casi no se implementa en las redes Ethernet.

PAR TRENZADO: Este es un tipo de cable que se utiliza para las comunicaciones telefónicas y la mayoría de las redes Ethernet modernas, en este cable los pares están trenzados para proporcionar protección contra la Diafonía, el ruido generado por pares adyacentes.
Los pares de hilos están trenzados por dos razones:

- La Cancelación: Es cuando un hilo lleva corriente y esta crea un campo magnético alrededor, este campo puede interferir con señales o con hilos cercanos. Para evitar esto se transportan señales en direcciones opuestas de modo que los campos magnéticos también se generan en campos opuestos y se neutralizan.
- Las Señales Diferenciales: suceden cuando por cada uno de los hilos se envía una copia de los datos, siendo las copias imágenes espejo de los datos.

Hay dos Tipos de Cable de Par Trenzado:

STP (Par Trenzado Blindado):

Este cable contiene cuatro pares de hilos de cobre cubiertos por unos aislantes plásticos codificados por colores y trenzados conjuntamente, cada par esta envuelto en una lamina metálica y los cuatro pares envueltos colectivamente con otra capa metaliza y recubierto con plástico en el exterior.

El cable SCTP es una variante del STP ya que lleva los mismos componentes que el cable STP pero con un adicional, el cual es una capa de blindaje alrededor de los cuatro pares de hilos. El blindaje en ambos tipos de cable STP reduce el ruido eléctrico indeseado.

Para instalar este cable se necesita que los blindajes metálicos estén conectados a tierra, si no se instalan correctamente este tipo de cables puede que fallen ya que son muy susceptibles a los problemas de ruido.

UTP (Cable de Par Trenzado Sin Apantallar):

Esta compuesto por cuatro pares de hilos de cobre finos cubiertos por unos aislantes plásticas codificados por colores y trenzados en conjunto, los pares de hilos están cubiertos por una carcasa plástica exterior. El conector utilizado en un cable UTP se denomina RJ-45.

Ventajas:

- Tiene un diámetro pequeño y no requiere conexión a tierra.
- Su tamaño supone una ventaja adicional, por que en una zona dada entra mucho más cable UTP que de otro tipo.
- Es el medio de red mas barato.
- El conector es más fácil de construir.
- Soporta las mismas velocidades de datos que otros medios de cobre.

Desventajas:

- Resulta susceptible al ruido eléctrico y las interferencias.
- La máxima longitud de tendido es inferior a la permitida por los cables coaxial y fibra óptica.

El cable UTP esta considerado como el medio basado en el cobre más rápido. Los cables UTP mas utilizados son los siguientes:

- **Categoría 1 (CAT 1):** Se utiliza para comunicaciones telefónicas, no es adecuado para la transmisión de datos
- **Categoría 2 (CAT 2):** Capaz de transmitir datos a velocidades superiores a 4Mbps.
- **Categoría 3 (CAT 3):** Se utiliza en redes Ethernet 10 BaseT, puede transmitir datos a velocidades de hasta 10 Mbps.
- **Categoría 4 (CAT 4):** Se utiliza en las redes Token Ring. Pueden transmitir datos a velocidades de hasta 16 Mbps.
- **Categoría 5 (CAT 5):** Puede transmitir datos a velocidades de hasta 100 Mbps. Se utiliza en redes Fastethernet.
- **Categoría 5e (CAT 5e)**: Se utiliza en redes con velocidades de hasta 1000Mbps, se usa en redes Gigabit Ethernet.
- **Categoría 6 (CAT 6):** Se utiliza en redes Gigabit Ethernet

10.1 NORMAS DEL CABLEADO

Existen muchas especificaciones para el cable a fin de asegurar interoperabilidad, seguridad y rendimiento. El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) han diseñado la especificación 802.3 que es la norma para las redes Ethernet.

La asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA) han emitido las siguientes normas sobre el cableado:

- TIA/EIA-586-B: Norma para el cableado de telecomunicaciones en un edificio comercial. Se centra en el cableado horizontal, que es el cableado que se extiende desde un enchufe de la pared del área de trabajo hasta un recinto de cableado.

- TIA/EIA-563-B: Norma para edificios comerciales para caminos y espacios de telecomunicaciones.
- TIA/EIA-568-A: Norma para edificios comerciales para el cableado de telecomunicaciones.
- TIA/EIA-568-B: Esta norma especifica los requisitos de componentes y transmisión para los medios. TIA/EIA-568-B.1 especifica un sistema genérico de cableado de telecomunicaciones para edificios comerciales que soportara un entorno multiproducto.
- TIA/EIA-569-A: Norma de edificios comerciales para recorridos y espacios de telecomunicaciones.
- TIA/EIA-570-A: Norma de cableado de telecomunicaciones comercial ligera y residencial.
- TIA/EIA-606-A: Norma de administración para la infraestructura de telecomunicaciones de edificios comerciales, incluyendo normas de etiquetado de cables.
- TIA/EIA-607: Para edificios comerciales conectados a tierra y con requisitos de enlace para telecomunicaciones. Considera un entorno multiproducto, multidistribuido, así como las prácticas de conexión a tierra para varios sistemas.

Reglas del Cableado Estructurado para LANs:

El cableado estructurado es un método sistemático de cableado. Es un procedimiento para crear un sistema organizado de cableado que puede ser entendido fácilmente por los inhaladores, los administradores de red y otros técnicos que trabajan con cables.

Hay tres reglas que ayudan a asegurar que los proyectos sean a la vez efectivos y eficaces:

1. Buscar una solución de conectividad completa: Esta incluye todos los sistemas diseñados para conectar, enrutar, administrar e identificar los sistemas de cableado estructurado. Utilizando las normas, ayudara a asegurar que las redes pueden soportarse tanto en las tecnologias actuales como en las futuras.
2. Plan para el crecimiento futuro: El número de circuitos debe considerarse a futuro y cumplir requisitos de redes proyectadas al futuro, se deben considerar los cables Cat6 y fibra óptica. Debe ser posible planificar una instalación de capa fisica que funcione diez años o más.
3. Mantener la libertad de elección de los distribuidores: Un sistema no estándar a partir de un solo distribuidor puede hacer más difícil efectuar movimientos, añadidos y cambios con posterioridad.

10.2 ESCALABILIDAD:

Es importante planificar una red con anticipación al estimar el número de recorridos de cable y derivaciones de cable en un área de trabajo. Siempre es fácil ignorar los cables extras instalados y no tener que instalar cuando se necesitan.

10.3 CASO DE ESTUDIO CAPA 1

Las instalaciones físicas de la empresa están compuestas por un edificio recientemente construido, el cual consta de dos plantas que van de la siguiente manera:

La planta del primer piso se encuentra dividida en tres partes:

- Operativa (Tornos, Fresas, Cortadora, Cepillo).
- Almacén de Materiales y Herramientas.
- Producción (Realización de planos).

En la planta del segundo piso se encuentra:

- Área Administrativa
- Área de Contabilidad
- Área de Compras y Ventas

Estas cuentan únicamente con tomas de conexión de red, líneas telefónicas y con un cableado eléctrico, el cual tiene polo a tierra en cada uno de sus puntos de conexión. El cableado de las conexiones de red, telefónicas y eléctricas se encuentran en el mismo ducto dentro de la pared.

Se requiere organizar el cable en canaletas, cada una con su punto de conexión a red, teléfono y electricidad; ya que actualmente solo se cuenta con 6 puntos en el segundo piso y 4 puntos en el primer piso, donde se encuentran las tomas anteriormente mencionadas, por lo tanto no son suficientes para las necesidades de la Empresa y de la Red.

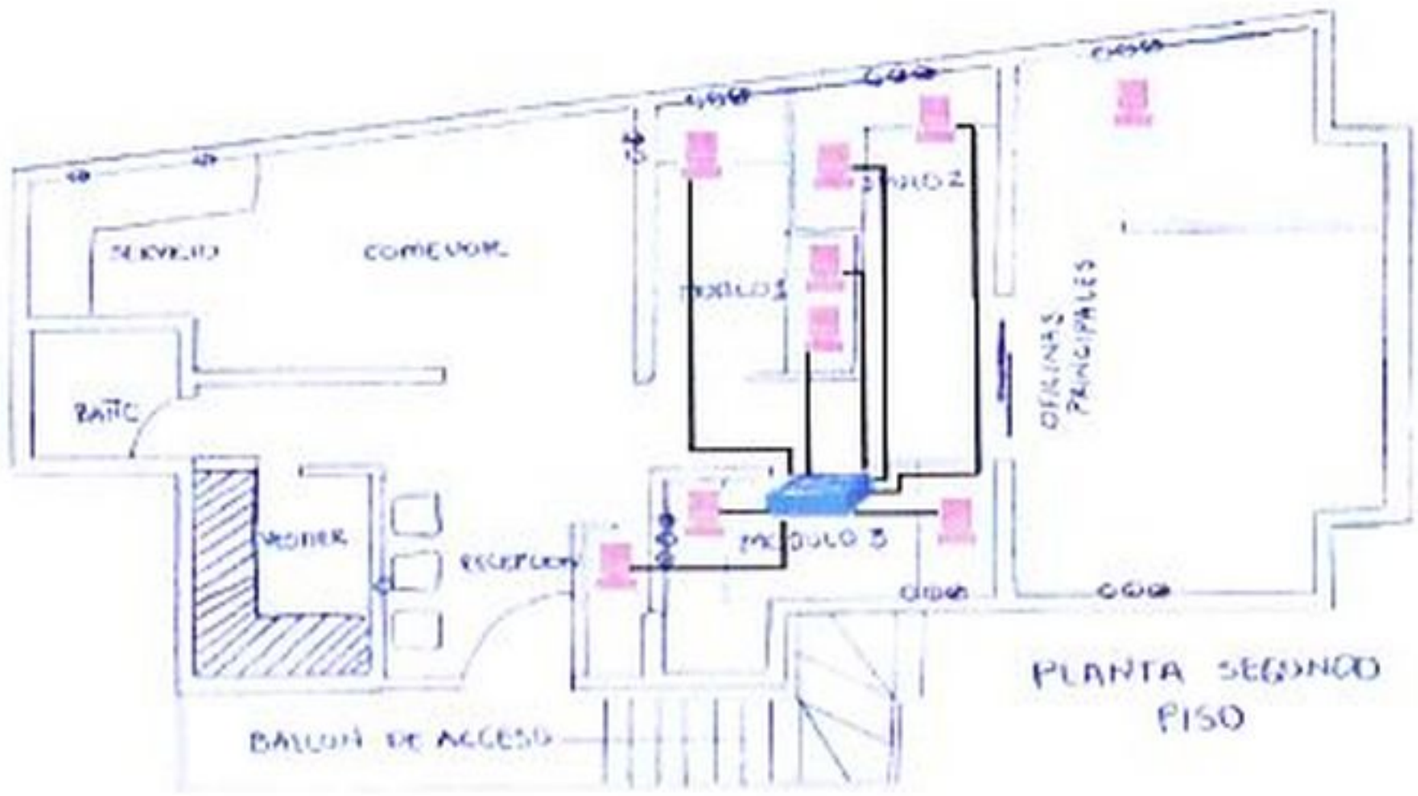
La sede también cuenta fisicamente con un sitio, el cual se utilizaría como cuarto de máquinas y se encuentra ubicado en el primer piso.

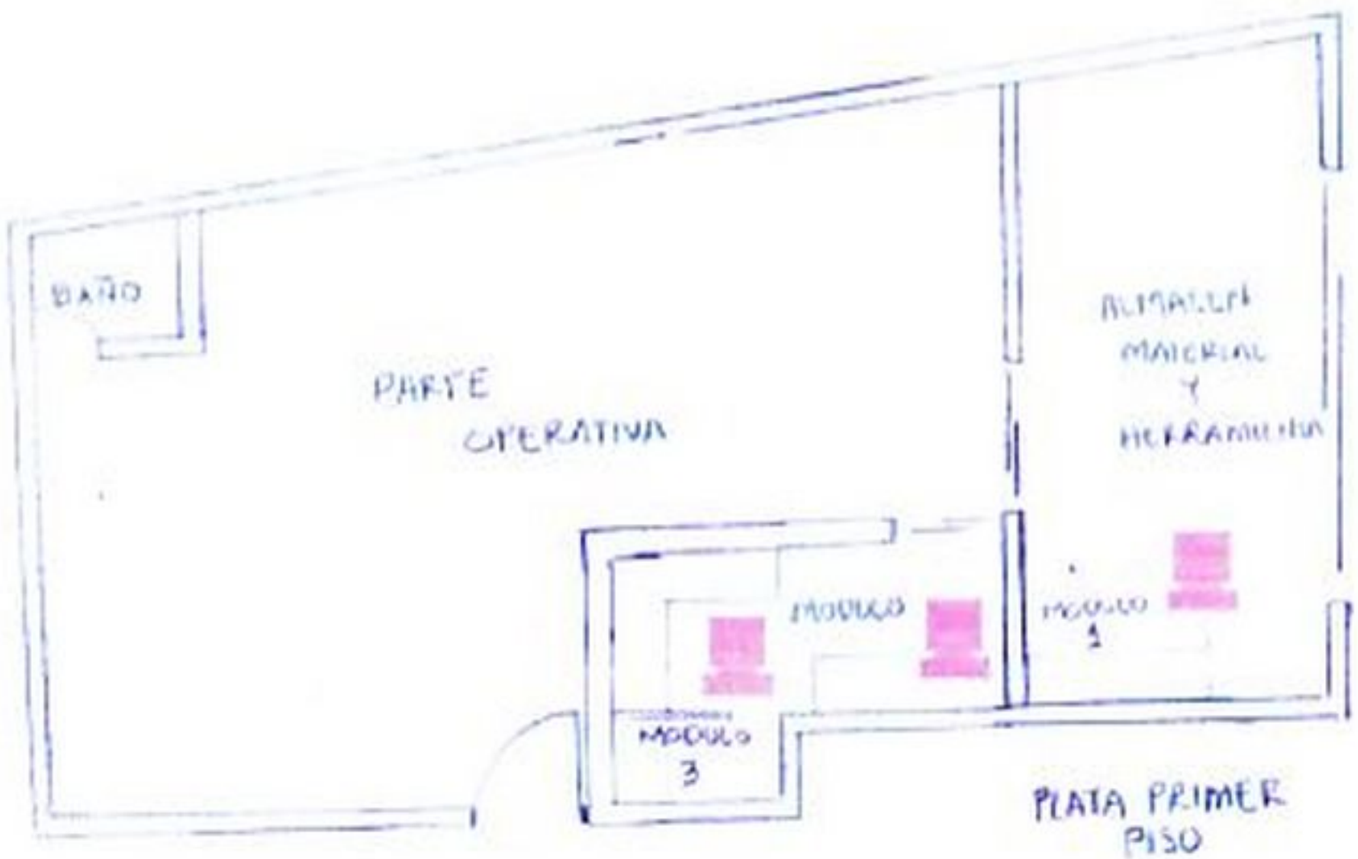
Actualmente cuenta con dos impresoras y doce estaciones de trabajo las cuales están ubicadas de la siguiente forma:

3 en el área Administrativa.
2 en el área de Contabilidad.
3 en el área de Compras y Ventas.
4 en el departamento de Producción.

Se verifica si el predio tiene disponibilidad para 20 estaciones de trabajo, ya que por disposiciones de la directiva se requiere esta cantidad, por el crecimiento de la empresa no les es suficiente para suplir sus necesidades.

10.4 MAPA FISICO ACTUAL





Entre los ejemplos de dicha información se incluye:

- Cuáles son los Computadores que se comunican entre si.
- Cuándo comienza y cuándo termina la comunicación entre computadores individuales.
- Proporciona un método para detectar los errores que se produjeron durante la comunicación.
- Quién tiene el turno para "hablar" en una "conversación" entre computadores

El entramado es el proceso de encapsulamiento de la Capa 2. Una trama es la unidad de datos del protocolo de la Capa 2.
Hay varios tipos distintos de tramas que se describen en diversos estándares. Una trama genérica tiene secciones denominadas campos y cada campo está formado por bytes. Los nombres de los campos son los siguientes:

- Campo de inicio de trama
- Campo de dirección
- Campos de longitud/tipo
- Campo de datos
- Campo de secuencia de verificación de trama

Cuando los computadores se conectan a un medio físico, debe existir alguna forma de informar a los otros computadores cuando están próximos a enviar una trama. Las diversas tecnologías tienen distintas formas para hacerlo, pero todas las tramas, de cualquier tecnología, tienen una secuencia de señalización de inicio de bytes.

Todas las tramas contienen información de denominación como, por ejemplo, el nombre del computador origen (dirección MAC) y el nombre del computador destino (dirección MAC).

La mayoria de las tramas tienen algunos campos especializados. En algunas tecnologias, el campo "longitud" especifica la longitud exacta de una trama en bytes. Algunas tienen un campo "tipo", que especifica el protocolo de Capa 3 que realiza la petición de envio.

La razón del envio de tramas es hacer que los datos de las capas superiores, especialmente los datos de aplicación del usuario, lleguen desde el origen hasta el destino. El paquete de datos incluye el mensaje a ser enviado, o los datos de aplicación del usuario. Puede resultar necesario agregar bytes de relleno de modo que las tramas tengan una longitud mínima para los fines de temporización. Los bytes de control de enlace lógico (LLC) también se incluyen en el campo de datos de las tramas del estándar IEEE. La subcapa LLC toma los datos de protocolo de la red, un paquete IP, y agrega información de control para ayudar a entregar ese paquete IP al nodo de destino. La Capa 2 se comunica con las capas de nivel superior a través de LLC.

Hay tres tecnologías muy utilizadas en capa 2 las cuales son:

- **Token Ring:** Topología de Anillo Lógica, la información fluye controlada en un anillo y también en Topología de Estrella Física.
- **FDDI:** Topología en Anillo Lógica y topología en anillo doble.
- **Ethernet:** Topología de Bus Lógica y Estrella Física o Extendida.

TECNOLOGÍA FDDI:

Norma LAN definida por el instituto nacional americano de normalización (ANSI), que especifica que una red de paso de testigo a 100 Mbps utilizando cable de fibra óptica con una distancia de transmisión superior a 2 Km.
La FDDI utiliza una arquitectura anillo doble para proporcionar redundancia.

TECNOLOGÍA TOKEN RING:

LAN de paso testigo, esta funciona a 4 ó 16 Mbps sobre una topología en anillo. Pueden conectarse hasta 72 dispositivos si se utiliza un cable telefónico estándar. Con cables de par trenzado apantallados, la red permite hasta 260 dispositivos. A pesar de que está basada en una topología de anillo (de bucle cerrado), la red Token Ring emplea segmentos en forma de estrella de hasta 8 estaciones de trabajo, conectadas a un concentrador de cableado, que a su vez se conecta al anillo principal. La red Token Ring está diseñada para su uso con microordenadores o microcomputadoras, minicomputadoras y mainframes. Sigue el estándar IEEE 802.5 para redes Token Ring

TECNOLOGÍA ETHERNET:

Ethernet es una tecnología de difusión de medio compartido. El método que se emplea en ethernet CSMA/CD realiza tres funciones:

- Transmitir y recibir paquetes de datos
- Decodificar paquetes de datos y comprobar las direcciones válidas antes de pasarlos a las capas superiores del modela OSI.
- Detectar errores en los paquetes de datos o en la red.

En el método de acceso CSMA/CD, los dispositivos de red con datos para transmitir por lo medios de red trabajan de modo "escuchar antes de transmitir" (CS: detección de portadora), en Ethernet esto significa que cuando un dispositivo quiere enviar datos, primero debe comprobar si el medio de red esta ocupado. Después debe comprobar dónde hay señales en el medio de red y finalmente si el medio de red no está ocupado, comenzar a retransmitir los datos. Mientras se transmiten los datos el dispositivo también escucha para asegurarse que ninguna otra estación está transmitiendo datos por el medio de red al mismo tiempo, ya que si esto sucede ocurriría una colisión; cuando ha finalizado la transmisión de datos, el dispositivo vuelve al modo de escucha.

Los dispositivos de red son capaces de detectar cuándo se ha producido una colisión, ya que aumenta la amplitud de la señal de los medios de red (CD:

detección de colisión). Cuando se produce una colisión, cada dispositivo que transmite continúa transmitiendo datos durante un corto espacio de tiempo, para asegurarse de que todos los dispositivos ven la colisión. Cuando todos los dispositivos la han visto, cada dispositivo transmisor llama a un algoritmo, conocido como Algoritmo de retardo. Cuando todos los dispositivos de la red se han retardado durante un cierto periodo de tiempo, cualquier dispositivo puede intentar de nuevo el acceso a la red. Cuando la transmisión de datos continua, los dispositivos que se han visto involucrados en la colisión no tienen prioridad.

Ethernet es una tecnología de transmisión por difusión, ósea que todos los dispositivos de una red pueden ver todas las tramas que pasan por los medios de red. Solo los dispositivos cuyas direcciones MAC coinciden con las direcciones MAC de destino transportadas por las tramas copian la traman en su buffer.

Ethernet no se preocupa por direcciones de red de la capa 3.

Ethernet es una arquitectura de Red Sin Conexión y se conoce como sistema de máximo esfuerzo de entrega.

Hay situaciones que se consideran errores Ethernet las cuales son:

- La transmisión simultánea se produce antes de que el tiempo de ranura haya transcurrido. (Colisión)
- La transmisión simultanea se produce después de transcurrido el tiempo de ranura (Colisión atrasada)
- Transmisión excesiva o ilegalmente larga (error, trama larga y errores de rango)
- Transmisión ilegalmente corta (trama corta, fragmento de colisión)
- Transmisión corrupta (error FCS)
- Numero de bits transmitido insuficiente o excesivo (error de alineación)
- Desigualdad en el número de octetos de la trama actual y el informado (error de rango).
- Preámbulo inusualmente largo o evento de congestión.

COLISIONES:

Las colisiones normalmente tienen lugar cuando dos o más estaciones Ethernet transmiten simultáneamente dentro de un dominio de colisión. La mayoria de las herramientas de diagnostico informan de las colisiones mediante cómputos de eventos, pero también pueden informar de forma separada como colisiones sencillas, o como varias colisiones cuando a un switch u otra estación se le preguntan con SNMP. (Protocolo Simple de Administración de Redes). Una colisión sencilla es una colisión detectada mientras se intenta transmitir una trama, pero al siguiente intento, la trama se ha transmitido bien.

Varias colisiones indican que la misma trama colisiona repetidamente antes de ser transmitida correctamente.

TIPOS DE COLISIONES:

Los principales tipos de errores son la colisión local, la colisión remota y la colisión atrasada.

- Colisión Local: Para crear una colisión local en un cable coaxial (10 Base2 y 10 Base5), la señal viaja por el cable hasta que se encuentra una señal de otra estación. Las ondas entonces se solapan, cancelando algunas partes de la señal y reforzando (doblando) otras. El doblado lleva el nivel del voltaje más allá del máximo permitido. Todas las estaciones en el segmento de cable local sienten esta condición de sobretensión como una colisión.
- Colisión Remota: Las caracteristicas de la colisión remota son una trama que tiene menos de la longitud minima y tiene una suma de comprobación FCS no válida, y además no exhibe síntomas de colisión local, de sobretensión o de una actividad RX/TX simultánea.
- Colisión Atrasada: Son las colisiones que ocurren después de los primeros 64 octetos. La NIC Ethernet transmite automáticamente una trama conflictiva, pero no transmite automáticamente una trama que colisione mas tarde.

SEGMENTACION:

Conectar varias computadoras a un medio de acceso compartido que no tiene otros dispositivos de red conectados crea un dominio de colisión esta situación limita el número de computadoras que pueden emplear el medio, también conocido como segmento.

Los dispositivos de capa 2 segmentan o dividen los dominios de colisión, controlando la propagación de la trama, empleando la dirección MAC asignada a cada dispositivo Ethernet, se realiza esta función. Los dispositivos de capa 2 como puentes y switches hacen un seguimiento de las direcciones MAC y del segmento donde están. Al hacer esto los dispositivos pueden controlar el flujo del trafico al nivel de la capa 2, esta función hace que las redes sean mas eficientes, al permitir que los datos se transmitan al mismo tiempo a diferentes segmentos de la red LAN, sin que colisionen las tramas. Al emplear puentes y switches el dominio de colisión se divide eficazmente en

partes más pequeñas, siendo cada una de ellas su propio dominio de colisión.

Estos dominios de colisión más pequeños tienen menos host y menos tráfico que el dominio original y por consiguiente aumenta la cantidad de ancho de banda disponible para cada host en el dominio. Cuanto menor sea la cantidad de tráfico en un dominio de colisión, mayor es la posibilidad de que cuando un host quiera transmitir datos, el medio esté disponible. Esto funciona bien mientras el tráfico entre segmentos no sea excesivo. En caso contrario los dispositivos de capa 2 pueden realizar realmente la comunicación y convertirse ellos mismos en un cuello de botella de la red.

11.1 EQUIPOS DE CAPA 2

11.1.1 TARJETAS DE INTERFAZ DE RED (NIC):

Cada tarjeta tiene un código denominado dirección de control de acceso al medio (MAC), dicha dirección controla el acceso del host al medio. Es una placa de circuito impreso que proporciona capacidades de comunicación de reda hacia y desde un PC. También conocida como adaptador de LAN, se conecta la placa madre y proporciona un puerto para conectarse a la red. La NIC constituye la interfaz de la computadora con la LAN.

11.1.2 PUENTES:

Dispositivo diseñado para crear dos o más segmentos LAN, cada uno de ellos con un dominio de colisión separado. Es decir que han sido diseñados para crear un ancho de banda más utilizable. El propósito de un puente es filtrar el tráfico de la LAN para mantener el tráfico local, permitiendo la conectividad con otras partes (segmentos) de la red LAN para el tráfico que se dirige alli. Cada dispositivo de la red tiene una dirección MAC única en al NIC. El puente control que direcciones MAC tiene en cada lado del puente y toma sus decisiones basándose en la lista de direcciones MAC. Los puentes pueden enviar rápidamente tráfico representando cualquier protocolo de la capa de RED, como los puentes solo se fijan en las direcciones MAC no se
preocupan por los protocolos de la capa de red. Las propiedades más importantes de los puentes son:

- Recolectan y pasan paquetes entre dos o más segmentos de la red LAN.
- Crean mas dominio de colisión, permitiendo que más de un dispositivo pueda retransmitir simultáneamente sin provocar una

colisión.

- Mantiene las tablas de direcciones MAC.

11.1.3 SWITCHES:

Son conocidos como switches de grupo de trabajo ó conmutadores, a menudo sustituyen a los hubs compartidos y trabajan con las infraestructuras de cables existentes para garantizar que los switches estén instalados con el mínimo de alteración de las redes existentes.

Estos permiten interconectar múltiples segmentos LAN físicos en redes sencillas más grandes. De forma similar a los puentes los Switches remiten e inundan el tráfico en base a las direcciones MAC. Como la conmutación se lleva a cabo en el hardware, es significativamente más rápido que la función de conmutación la realice un puente utilizando software. Cada puerto del switch actúa como un puente separado y proporciona a cada host el ancho de banda completo del medio. Este proceso se conoce como microsegmentación.

La microsegmentación permite la creación de segmentos privados o dedicados: un host por segmento. Cada host recibe acceso instantáneo al ancho de banda completo y no tiene que competir con otros host por un ancho de banda disponible. En los switches duplex, como solo un dispositivo está conectado a cada uno de los puertos del switch no se producen colisiones. Sin embargo como ocurre con un puente, un switch remite un mensaje de difusión a todos los segmentos de este, por consiguiente se considera que todos los segmentos en un entorno conmutado están en el mismo dominio de colisión.

11.2 CASO DE ESTUDIO CAPA 2

La topología que existe entre los ocho computadores conectados es en forma de estrella, ya que se encuentra unida por un punto de conexión central, el cual es un switch, en donde cada uno de los PCs están conectados a él con su propio cable.

El switch utilizado actualmente en la red es de Marca Encore Electronics, Ref. ENH908-NWY, es un interruptor rápido de alto rendimiento de Ethernet con 8 puertos capaces de las velocidades hasta de 100Mbps. la autonegociación se determina automáticamente entre 10Mbps o 100Mbps, al conectar con otros dispositivos del establecimiento de una red. Usando cables de categoría 5 (RJ-45), esta unidad puede funcionar en modo Full-duplex o Half-duplex, permitiendo conectividad a las enrutadores, a las tarjetas de red y a otros interruptores.
Únicamente tiene funciones de conmutar ya que no es administrable.

Los Puertos de los PC son Ethernet.

12. CAPA DE RED

La capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (la PDU de la Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como, por ejemplo, las direcciones lógicas origen y destino.

El principal componente de esta capa de red es el Router que provee enrutamiento y elige la mejor ruta, por medio de protocolos.

PROTOCOLOS

ENRUTADOS:

IP:

El protocolo Internet es un enrutable que funciona en la capa de red del modelo OSI y en la capa de Internet del modelo TCP/IP. Proporciona entrega de paquetes y direccionamiento para el origen y el destino.

Este es un protocolo del sistema de máximo esfuerzo de entrega, poco fiable sin conexión que se utiliza en Internet. El término sin conexión significa que no es necesaria la conexión de circuito dedicada, este protocolo toma cualquier ruta que sea más eficaz en base a la decisión del protocolo de enrutamiento. "Poco fiable" y "máximo esfuerzo" no significa que el sistema sea poco fiable y que no funcione bien, sino que el protocolo IP no hace ningún esfuerzo por ver si el paquete fue entregado.

IP determina la forma de la cabecera del paquete IP (que incluye

direccionamiento y otra información de control), pero no se preocupa de los datos reales. Acepta cualquier cosa que pase hacia abajo desde las capas superiores.

IPX:

Es un protocolo enrutable sin conexión que también funciona en la capa de red del modelo OSI. IPX es eficaz, no plantea problemas a nivel de rendimiento ni de direccionamiento y es posible emplearlo en redes Ethernet y Token Ring utilizando los controladores de tarjeta de interfaz de red (NIC) adecuados.

APPLE TALK:

AppleTalk es una red de banda base que transfiere información a una velocidad de 230 kilobits por segundo y enlaza hasta 32 dispositivos (nodos) en una distancia de aproximadamente 300 metros mediante un conductor doble trenzado blindado denominado Local Talk, transmitiendo la información en forma de paquetes llamados tramas. AppleTalk es compatible con conexiones a otras redes AppleTalk a través de dispositivos llamados puentes y también con conexiones a redes diferentes mediante dispositivos denominados puertas de enlace.

ENRUTAMIENTO:

ICMP:

Protocolo de Mensajes de Control en Internet; es el protocolo encargado de asegurar la entrega de datos. ICMP no supera la falta de fiabilidad existente en IP, simplemente envía mensajes de error al emisor de los datos, indicando que se ha producido problemas en la entrega de los datos.

ARP:

Protocolo de Resolución de Direcciones; para que los dispositivos se comuniquen al dispositivo emisor necesita las direcciones IP y MAC del dispositivo destino. Cuando un dispositivo intenta comunicarse con otro dispositivo cuyas direcciones IP conoce, debe determinar las direcciones MAC. Este protocolo sirve para obtener automáticamente la dirección MAC de la computadora asociada con una dirección IP. Este protocolo anexa unas tablas ARP que contiene las direcciones MAC e IP de otros dispositivos conectados a la misma LAN.

RARP:

Protocolo de Resolución Inversa de Direcciones; une las direcciones MAC con la direcciones IP, esta unión permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red.

RIP:

Protocolo de Información de Enrutamiento; Protocolo que utiliza la cuenta de saltos para determinar la dirección y la distancia a cualquier enlace en la red, este selecciona la ruta con menos saltos, pero esto hace que no seleccione la ruta más rápida a un destino.

IGRP:

Protocolo de Enrutamiento de Gateway Interior; Protocolo de enrutamiento por vector distancia, esto significa que puede seleccionar la ruta más rápida en base al retardo, el ancho de banda, la carga y la fiabilidad. Utiliza una métrica de 24 bits.

EIGRP:

Es una versión avanzada de IGRP que proporciona eficiencia operativa superior, utiliza una métrica de 32 bits, como una convergencia más rápida y una menor sobrecarga del acho de banda. Este es un protocolo por vector distancia avanzado, también utiliza funciones de protocolo de estado de enlace.

OSPF:

Protocolo de Primero la Ruta Libre Más Corta; Protocolo de enrutamiento de estado de enlace basado en estándares abiertos, determina la mejor ruta y de coste mas bajo hacia el enlace.

EGP:

Protocolo de Gateway Exterior; es un protocolo de Internet utilizado para intercambiar información de enrutamiento entre sistemas autónomos.

12.1 TABLAS DE ENRUTAMIENTO

Los Routers utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas. Los dispositivos de Capa 3 interconectan dominios de Broadcast o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos.

Los Routers mantienen información importante en sus tablas de enrutamiento, que incluye lo siguiente:

- Tipo de protocolo: el tipo de protocolo de enrutamiento que creó la entrada en la tabla de enrutamiento.
- Asociaciones entre destino/siguiente salto: estas asociaciones le dicen al Router que un destino en particular está directamente conectado al Router, o que puede ser alcanzado utilizando un Router denominado "salto siguiente" en el trayecto hacia el destino final.
- Métrica de enrutamiento: los distintos protocolos de enrutamiento utilizan métricas de enrutamiento distintas. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta.
- Interfaces de salida: la interfaz por la que se envían los datos para llegar a su destino final.

Los Routers se comunican entre si para mantener sus tablas de enrutamiento por medio de la transmisión de mensajes de actualización del enrutamiento.

ALGORITMOS DE ENRUTAMIENTO Y MÉTRICAS

Un algoritmo es una solución detallada a un problema. En el caso de paquetes de enrutamiento, diferentes protocolos utilizan distintos algoritmos para decidir por cuál puerto debe enviarse un paquete entrante. Los algoritmos de enrutamiento dependen de las métricas para tomar estas decisiones.

Los protocolos de enrutamiento con frecuencia tienen uno o más de los siguientes objetivos de diseño:

- Optimización: la optimización describe la capacidad del algoritmo de enrutamiento de seleccionar la mejor ruta.
- Simplicidad y bajo gasto: cuanto más simple sea el algoritmo, más eficientemente será procesado por la CPU y la memoria del Router.

- Solidez y estabilidad: un algoritmo debe funcionar de manera correcta cuando se enfrenta con una situación inusual o desconocida.
- Flexibilidad: un algoritmo de enrutamiento debe adaptarse rápidamente a una gran variedad de cambios en la red.
- Convergencia rápida: la convergencia es el proceso en el cual todos los Routers llegan a un acuerdo con respecto a las rutas disponibles.

Los algoritmos de enrutamiento utilizan métricas distintas para determinar la mejor ruta. Cada algoritmo de enrutamiento interpreta a su manera lo que es mejor. Los algoritmos de enrutamiento sofisticados basan la elección de la ruta en varias métricas, combinándolas en un sólo valor métrico compuesto. Las métricas pueden tomar como base una sola característica de la ruta, o pueden calcularse tomando en cuenta distintas características. Las siguientes son las métricas más utilizadas en los protocolos de enrutamiento:

- Ancho de banda: la capacidad de datos de un enlace. En general, se prefiere un enlace Ethernet de 10 Mbps a una linea arrendada de 64 kbps.
- Retardo: la cantidad de tiempo requerido para transportar un paquete a lo largo de cada enlace desde el origen hacia el destino
- Carga: la cantidad de actividad en un recurso de red como, por ejemplo, un Router o un enlace.
- Confiabilidad: generalmente se refiere al índice de error de cada enlace de red.
- Número de saltos: el número de Routers que un paquete debe atravesar antes de llegar a su destino..
- Tictacs: el retardo en el enlace de datos medido en tictacs de reloj PC de IBM.
- Costo: un valor arbitrario asignado por un administrador de red que se basa por lo general en el ancho de banda, el gasto monetario u otra medida.

12.2 VLAN

Las VLAN son un grupo de dispositivos de red y servicios que no están restringiendo a un segmento fisico, agrupan un conjunto de usuarios en una misma red de forma lógica, estas se encargan de la escalabilidad, la seguridad y la administración de la red. Los router en las topologías VLAN proporcionan filtrado de difusión, seguridad y administración del flujo del tráfico.

Las VLAN segmentan lógicamente las redes conmutadas basándose en las funciones, equipos de proyecto o aplicaciones de una empresa, en lugar de hacerlos sobre una base fisica. Un ejemplo claro es cuando las estaciones de trabajo y servidores que utiliza un equipo de trabajo podria conectarse a la misma VLAN con independencia de sus conexiones fisicas a la red.

Una VLAN puede entenderse como un dominio de difusión existente dentro de un conjunto definido de Switches. Se crean para proporcionar los servicios de segmentación que normalmente ofrecen los routers en las configuraciones

Caracteristicas:

- Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN fisico.
- Las VLAN mejoran el desempeño general de la red agrupando a los usuarios y los recursos de forma lógica.
- Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento fisico de LAN.
- Facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.
- Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de

trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

La configuración o reconfiguración de las VLAN se logra mediante el software. Por lo tanto, la configuración de las VLAN no requiere que los equipos de red se trasladen o conecten físicamente. Una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores de archivo en el mismo grupo de VLAN. Las VLAN segmentan de forma lógica la red en diferentes dominios de

broadcast, de manera tal que los paquetes sólo se conmutan entre puertos y se asignan a la misma VLAN. Las VLAN se componen de hosts o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los switches de LAN operan protocolos de puenteo con un grupo de puente separado para cada VLAN.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

12.3 EQUIPOS CAPA 3

SERVIDORES:

Un servidor proporciona servicios de autenticación autorización y contabilidad para una empresa, estos servidores garantizan que los usuraos autenticados sean los únicos que tengan acceso a la red, que los usuraos solo tiene acceso a los recursos que necesitan y que se registra todo lo que ellos hacen después de permitir el ingreso a la red. Los servidores ofrecen servicio de compartir ficheros, impresión, comunicación y de aplicación, habitualmente estos dispositivos no funcionan como estaciones de trabajo y ejecutan sistemas operativos especializados. Cada servidor suele estar dedicado a una función especifica, como el correo electrónico ó compartir archivos.

Los servidores pueden ser clasificados como:

- **Servidores de Empresa:** Soporta todos los usuarios de la red ofreciendo como correo electrónico o de DNS. Estos son servicios que podrian ser necesarios para cualquier persona de esa organización porque son funciones centralizadas.; deben estar ubicados en armarios de distribución principal.
- **Servidores de Grupo de Trabajo:** Soporta a un conjunto de usuarios ofreciéndoles sólo aquellos servicios concretos que
pudiesen necesitar, deben estar en armarios de distribución intermedia, cercanos a los usuarios que utilizan las aplicaciones de dichos servidores.

ROUTERS:

Un router es un tipo de dispositivo de Internetworking que pasa paquetes de datos entre redes basándose en direcciones de la capa 3. Un router puede tomas decisiones acerca de la mejor ruta para la distribución de datos por la red, en lugar de utilizar direcciones MAC individuales de la capa 2. estos también pueden conectar deferentes tecnologías de capa 2 como Ethernet, Token Ring y FDDI.

Los router también se conectan con conexiones serie y ATM sin embargo a su capacidad de enrutar paquetes en base a la información de la capa 3, los routers se han convertido en el backbone de Internet y ejecutan el protocolo IP.

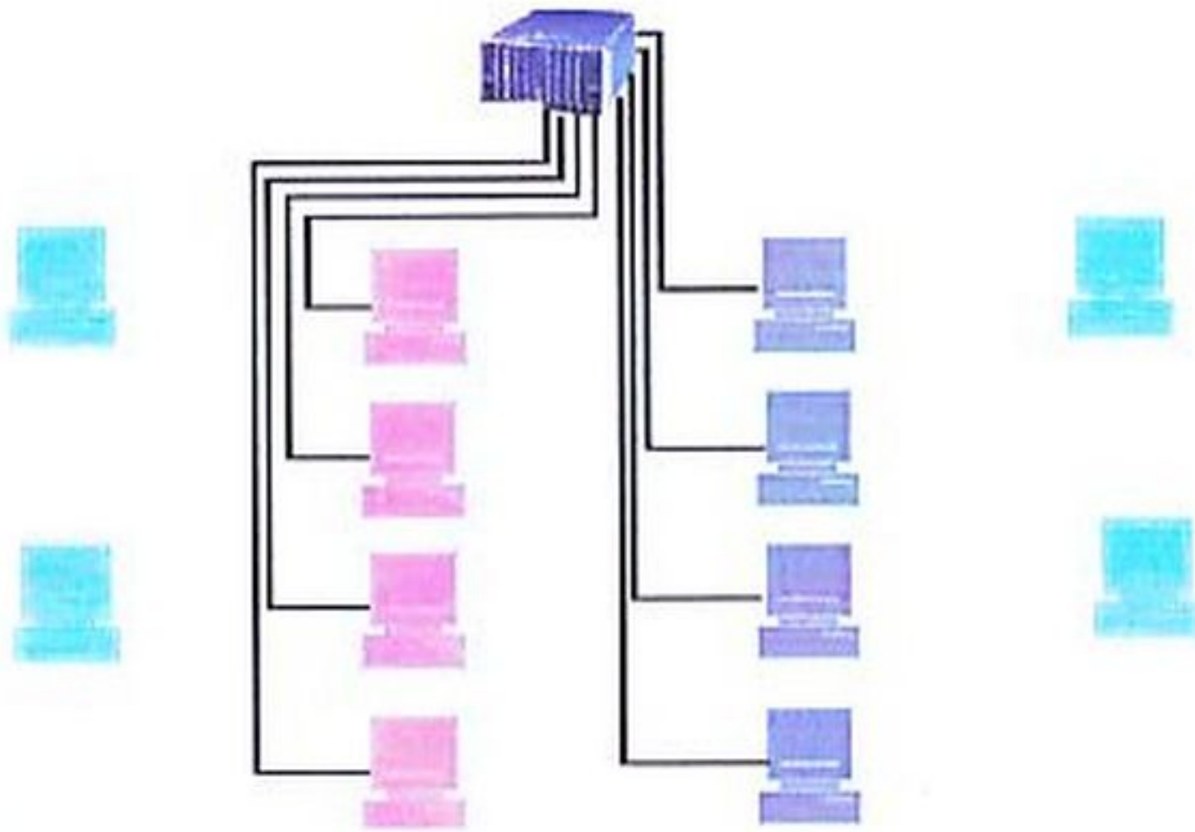
El propósito de un router es examinar los paquetes entrantes, elegir la mejor ruta para ellos a través de la red y después conmutarlos al puerto de salida apropiado. Los routers son el dispositivo regulador mas importante en la redes grandes, virtualmente permiten que cualquier tipo de computadora se comunique con otra en cualquier parte del mundo.LAN.

12.4 CASO DE ESTUDIO CAPA 3

Los PC no poseen direcciones IP establecidas para la red, solo registran las direcciones MAC.

Se utiliza conexión de Internet Conmutado por el proveedor Telecom, sólo 2 PCs tienen acceso a este servicio.
El ingreso es efectuado por IP Dinámica.

12.5 MAPA LOGICO ACTUAL



13. SEGURIDAD Y APLICACIONES

Para la protección de la red existen dos tipos de seguridad: la seguridad a nivel de los recursos y la seguridad a nivel de usuario. Catalogada como débil y dificil de manipular, la seguridad a nivel de los recursos permite a los usuarios acceder a cierta información si el administrador de la red les asigna una contraseña. Para que una persona acceda a la información de la red, ese usuario deberá proporcionar una contraseña, especificamente asignada por el administrador de red.

La seguridad a nivel de usuario especifica los derechos y privilegios de cada usuario. El administrador de red asigna una cuenta al usuario para que acceda a una computadora o red concretas. Cuando una persona trata de iniciar sesión en la red, la computadora compara el ID de cuenta del usuario y la contraseña con la base de datos de seguridad antes de proporcionar acceso al usuario.

Muchos protocolos se utilizan para cifrar datos y asegurar el tráfico entrante y saliente a través de la red. Algunos de los protocolos de seguridad mas populares son: IPSec, L2TP, SSL y Kerberos.

- **IPSec:** Es un conjunto de protocolos desarrollado para soportar el intercambio seguro de paquetes en la capa IP. Se ha desplegado ampliamente para implementar las VPN.
- **L2TP:** Es una extensión del protocolo PPP que habilitan los IPS para poder utilizar las VPN.
- **SSL:** Es un protocolo desarrollado por Netscape para la transmisión de documentos privados a través de Internet. Funciona utilizando una clave pública para cifrar los datos que se transfieren por la conexión SSL.
- **Kerberos:** Es un sistema de autenticación. Está diseñado para que las dos partes puedan intercambiar información privada a través de una red abierta distinta. Funciona asignando una clave única, denominada TICKET, a cada uno de los usuarios que inicia sesión en la capa de red.

Después, el ticket se incrusta en los mensajes para identificar el emisor del mensaje.

Antes de instalar una red, deberá tener en cuenta las configuraciones, la ubicación física, las topologías, la estructura física de la red, las obligaciones administrativas, las contraseñas, el direccionamiento IP, la configuración IP, los requisitos de conectividad y el Software.

Cuando se utiliza una cuenta administrativa para hacer cambios en la red, debe utilizar una cuenta de prueba y verificar los cambios. Las cuentas de prueba son parecidas a las de una cuenta de usuario normal y se asemejan a otras cuentas y privilegios de usuario.

Es necesario tener en cuenta los factores medioambientales a la hora de crear una red. Las computadoras y los dispositivos de red pueden verse afectados muy fácilmente por las situaciones extremas, como la temperatura, la humedad, las vibraciones y las interferencias eléctricas. Si se exponen a estas situaciones, las computadoras y los dispositivos de red podrían comportarse de forma irregular y fallar.
Las condiciones de la habitación o sala deben estar a una temperatura y humedad normales para prevenir las descargas eléctricas y el sobrecalentamiento. Los lugares frescos y oscuros, como los sótanos, son ideales para almacenar equipo computacional.

Procedimientos estándar de contraseña:

Las contraseñas deberán estar siempre en un lugar seguro y no deberán figurar en ningún sitio donde los usuarios las puedan descubrir.

Las contraseñas no deberán ser nada de lo siguiente:

1. El nombre de inicio de sesión, el nombre o los apellidos del usuario o estos nombres al revés.
2. Un nombre conocido, como el nombre de la esposa, hijo, mascota o familiar.
3. Datos fácilmente accesibles, como datos personales.
4. Una palabra que se encuentre en algún diccionario.
5. Únicamente una combinación de letras y números.
6. Un grupo de dígitos o letras iguales.

Las contraseñas deberán tener estas características:

1. Tener una longitud de entre seis y ocho caracteres.
2. Incluir caracteres no alfanuméricos.
3. Estar configuradas para que expiren periódicamente, idealmente cada 30 días.

Cifrado de datos:

El cifrado de datos proporciona la entrega segura de la información que se envía a través de Internet. Toma los datos, que están escritos en texto sin formato y los codifica en un texto, llamado Texto Cifrado, que no se parece a nada, lo que le convierte en ilegible. Cuando se reciben los datos, son descifrados del texto cifrado y convertidos nuevamente a su texto original.

El uso de un Firewall:

Un Firewall se emplea para proteger la red interna de Internet. Pueden ser implementados mediante Hardware y Software.

El Firewall Software es un conjunto de programas del Gateway que controla todo el tráfico que fluye por la red; suelen implementarse utilizando Routers configurados específicamente.

El Firewall Hardware es el uso de Routers configurados especialmente para controlar el tráfico de entrada y salida.

13.1 ROUTERS:

Un Router es un dispositivo que proporciona la selección de la mejor ruta y la conmutación de paquetes de datos. Para conectar dos redes distintas, hay que usar un Router. Se pueden utilizar para segmentar las LAN, creando dominios de colisión mas pequeños, pero el uso mas importante es, como dispositivos backbone de las WAN.

Pueden ser estáticos o dinámicos y normalmente se conectan en una topologia en malla con otros Routers.

13. 2 LISTAS DE CONTROL DE ACCESO (ACL):

Una ACL es una colección secuencial de sentencias de permiso o denegación que se aplica a las direcciones o los protocolos de la capa superior.

Son listas de instrucciones que puede aplicar a la interfaz del router. Estas listas le indican al router que tipo de paquetes aceptar y cuales denegar. La aceptación y denegación se pueden basar en ciertas especificaciones, como la dirección de origen, la dirección de destino y el número del puerto TCP/UDP.

Al aplicar la ACL a una interfaz del router puede administrar el tráfico y revisar los paquetes. Todo tráfico que pasa por la interfaz se compara con ciertas condiciones de la ACL.

Se pueden crear para todos los protocolos de red enrutados, como IP e IPX, para filtrar los paquetes que pasan por el router.

Las razones para crear ACL, son:

1. Limitar el tráfico de la red e incrementan su rendimiento.
2. Controlar el flujo del tráfico.
3. Proporcionar un nivel básico de seguridad para el acceso a la red.
4. Decidir que tipo de tráfico es enviado o bloqueado en la interfaz del router.

13.3 NAT y PAT:

NAT es un proceso de manipulación de direcciones en la cabecera IP de un paquete para que la dirección de destino, la de origen o ambas se sustituyan en dicha cabecera por otras direcciones asignadas por un administrador. Esta operación la lleva a cabo un dispositivo especial que dispone de Software o Hardware NAT especializado para este intercambio.
Un dispositivo con caracteristicas NAT opera habitualmente en el borde de una red de conexión única. La característica principal de las mismas es que dispone de una sola conexión con su red vecina.
NAT opera en un router, conectando dos redes y traduce las direcciones privadas de la red interna (Locales Internas) en direcciones públicas (Globales Internas) antes que los paquetes se envíen a otra red.

PAT usa números de puerto origen únicos en la dirección IP Global Interna para distinguir las diferentes conexiones. Ya que estos números de puerto están codificados en 16 Bits, la cantidad total de direcciones internas que pueden convertirse en una dirección externa usando PAT podría llegar teóricamente a 65.536 por IP.
PAT intenta preservar el puerto de origen original. Si este valor ya está asignado intenta encontrar el primer número de puerto disponible comenzando por el principio del grupo de puerto adecuado. En caso que esta condición no pueda cumplirse y este configurada mas de una dirección IP externa, PAT se

desplaza hacia la siguiente dirección IP e intenta asignar de nuevo el puerto de origen original. Este proceso continua hasta que PAT termine con todos los puertos y direcciones IP externas disponibles.

Caracteristicas:

1. Dirección Local Interna: La dirección IP asignada a un host en la red interna que es probable que sea una dirección privada.
2. Dirección Global Interna: Una dirección IP legitima que asigna el RIR (Registro de Internet Regional).
3. Dirección Local Externa: La dirección IP de un host externo que es conocidos por los hosts de la red interna.
4. Dirección Global Externa: La dirección IP que el propietario del host le asigna en la red externa.

Beneficios:

1. Elimina la sobrecarga de direccionamiento, como cambiar un ISP.
2. Conserva las direcciones mediante la aplicación de multiplexión en el ámbito de puerto.
3. Protege la seguridad de la red.

Ventajas:

1. Conserva el esquema de direccionamiento registrado legalmente permitiendo la privatización de Intranets.
2. Incrementa la flexibilidad de conexión a la red pública. Para ayudar a asegurar conexiones de red públicas fiables pueden implementarse varios almacenes, almacenes Backup y almacenes de carga compartida/equilibrada.

3. La desprivatización de una red requiere la renumeración de la red existente; el coste puede estar asociado con el número de hosts que requieren conversión al nuevo esquema de direccionamiento.

Desventajas:

1. Incrementa el retardo.
2. Se hace mucho más difícil seguir la pista de los paquetes que sufren numerosos cambios en su dirección, debido a sus múltiples saltos.
3. Obliga a algunas aplicaciones que usan direccionamiento IP a detener su funcionamiento porque oculta las direcciones IP extremo a extremo.

Aplicaciones:

1. ICMP.
2. FTP (Protocolo de Transferencia de Archivos).
3. NetBios sobre TCP/IP.
4. RealAudio.
5. DNS.
6. NetMeeting.
7. VDOLive.
8. Vxtreme
9. IP Multifusión.

13.4 ADMINISTRACIÓN DE REDES:

Según la red crece y evoluciona, se convierte en un recurso más crítico e indispensable para la organización. Sin embargo, cuanto mas recursos ofrece la red a sus usuarios y mas compleja se vuelve la red, son mas las cosas que pueden ir mal. Pero claro, la pérdida de recursos o incluso un rendimiento pobre de la red, no es algo aceptable por parte de esos mismos usuarios. El

administrador de la red debe controlarla de forma activa, diagnosticar sus problemas, prevenir las situaciones que puedan ocurrir y ofrecer le mejor rendimiento de la misma. En algún momento, las redes se hacen tan grandes que su control resulta muy dificil sin herramientas automatizadas.

Las tareas de administración de la red, incluyen lo siguiente:

1. Monitorizar la disponibilidad de la red.
2. Mejorar la automatización.
3. Monitorizar el tiempo de respuesta.
4. Seguridad.
5. Redirección del Tráfico.
6. Capacidad de restablecimiento.
7. Registro de usuarios.

Aspectos Básicos:

1. Controlar medios corporativos: Sin un control efectivo de los recursos de la red dichos recursos no ofrecerán el rendimiento preciso.
2. Control de complejidad: Con el importante crecimiento que sufren las redes en el número de componentes, usuarios, interfaces, protocolos y vendedores, la pérdida de control de la misma y de sus recursos es una amenaza para la administración.
3. Mejora del servicio: Los usuarios esperan el mismo rendimiento, o incluso mejor, según la red crece y los recursos se distribuyen de forma más adecuada.
4. Balanceo de diversas necesidades: Los usuarios deben disponer de diferentes aplicaciones para un nivel de soporte dado, con una especial atención a las áreas de rendimiento, disponibilidad y seguridad.
5. Reducción de los tiempos muertos: Asegurar una disponibilidad elevada de los recursos gracias al propio diseño redundante.

6. Control de Costes: Monitorizar y controlar la utilización de los recursos para que los usuarios estén satisfechos a un coste razonable.

Mantenimiento y Soporte de la Red:

Las actualizaciones de software están diseñadas para mejorar el software en curso y para hacerlo mas potente. Normalmente, las actualizaciones son gratuitas y pueden descargarse de la página Web del fabricante. No obstante, conviene hacer una copia de seguridad antes de la instalación para prevenir la pérdida de datos.

Si no hay software antivirus instalado en los servidores y estaciones de trabajo, ningún MODEM funcionará eficazmente. Dependiendo de las necesidades del usuario, existe una amplia gama de paquetes antivirus. Una estrategia de mantenimiento de red continuado debe incluir la actualización frecuente de los antivirus. Dado que cada vez aparecen más virus, en unos pocos meses, lo que era un software antivirus eficaz se puede convertir en algo obsoleto.

Todo administrador que mantenga una red debe disponer de un procedimiento estándar de copia de seguridad que ponga en práctica de noche. Entre los procedimientos de duplicación se deben incluir las unidades de cinta, la automatización de cinta y las copias de seguridades completas, incrementales y diferenciales.

Es importante parchear el software que se ejecuta en la estación de trabajo cliente y el propio servidor. Siempre hay software en el cliente que no está en el servidor y viceversa; si se actualiza o parchea el software en un servidor y no en una estación de trabajo, se podrian presentar problemas cuando los usuarios traten de acceder al software con una versión diferente.

Como solucionar problemas en la red:

1. Determinar si el problema afecta a toda la red.
2. Trate de aislar el problema.
3. Determine si el problema es permanente.
4. Determine si es posible resolver los problemas con el uso de herramientas.
5. Comprobar indicadores fisicos y lógicos del problema.

13.5 CASO DE ESTUDIO SEGURIDAD Y APLICACIONES

Los tipos de aplicaciones que utiliza la empresa son:

- Programa Contable Helisa 40 y Programa de Contabilidad Visual.
- Programa para realización de plano Autocad, Adobe Acrobat 6.0.2.
- Programa para visualización de planos recibidos: Macromedia Flash Player
- Programa para comprimir archivos: Winrar.

El sistema operativo que maneja la empresa es Windows XP.

Para seguridad únicamente cuenta con el Antivirus McAfee Virus Scan y los Firewalls de Windows.

14. PROPUESTA

A continuación daremos a conocer las caracteristicas de la solución LAN propuesta, acorde con las necesidades en la instalación de la Red Fisica y Lógica de la empresa Metaliza Ltda.

- **TOPOLOGÍA FISICA DE LA RED:**

Se propone crear la Topología en Estrella Extendida que esta diseñada con un punto de conexión central el cual será un Switch, donde se encuentra la segmentación del cable ya que cada Host o dispositivo adicional, estará conectado a este por su propio cable, así cuando exista algún problema con este, solo se vera afectado el Host que lo este implementando, no afectará a la red en general y podrá permanecer operando eficazmente.

- **TIPO DE CABLE:**

Se propone implementar Cable de Par Trenzado Sin Apantallar (UTP), el cual esta compuesto por cuatro pares de hilos de cobre, cubiertos por unos aislantes plásticos codificados por colores y trenzados en conjunto.

Ventajas:

- Tiene un diámetro pequeño y no requiere conexión a tierra.
- Su tamaño supone una ventaja adicional, por que en una zona dada entra mucho más cable UTP que de otro tipo.
- Es el medio de red mas barato.
- El conector es más fácil de construir.
- Soporta las mismas velocidades de datos que otros medios de cobre.

Desventajas:

- Resulta susceptible al ruido eléctrico y las interferencias.

- La máxima longitud de tendido es inferior a la permitida por los cables coaxial y fibra óptica.

- **CATEGORÍA DEL CABLE:**

Se utilizara cable UTP Cat6, ya que puede transmitir datos a velocidades de hasta 1 Gb.

- **MEDIOS DE CONEXIÓN:**

- RJ-45: Este conector se utiliza para finalizar un cable de par trenzado.
- AUI: este conector enlaza una NIC de computadora o una interfaz de un enrutador con un cable Ethernet.

- **DISPOSITIVOS DE CONEXIÓN LAN:**

- SWITCH CATALYST_24P
- ROUTER SOHO 91
- UPS BLAZER 2000 REGULADA
- RACK HP SHOCK PALLET

- **ESTACIONES DE TRABAJO:**

- La red contara con 20 estaciones de trabajo, dentro de las cuales estarán un servidor y 19 Host.
- Esta red estará habilitada para un mayor crecimiento.

- **TECNOLOGÍA DE ENLACE DE DATOS:**

Se propone implementar tecnología Ethernet ya que esta diseñada para compartir los recursos a nivel de grupo de trabajo en áreas pequeñas,

además que es muy simple de implementar, tiene poco retardo y una alta velocidad a la hora de transportar datos.

- **DIRECCIONAMIENTO IP:**

Se propone una dirección Clase C Privada y será del rango 192.168.16.0.

- **SEGURIDAD:**

Se propone utilizar usuarios y contraseñas en cada equipo, que la salida a Internet se realice la conversión NAT y configurar listas de acceso en el router.

14.1 CARACTERÍSTICAS DE LOS EQUIPOS:

1. **Switch Catalyst_24P:**

Memoria

Memoria RAM: 16 MB SDRAM

Memoria Flash: 8 MB Flash

Conexión de redes

Cantidad de puertos: 24 x Ethernet 10Base-T, Ethernet 100Base-TX

Velocidad de transferencia de datos: 100 Mbps

Protocolo de interconexión de datos: Ethernet, Fast Ethernet

Protocolo de gestión remota: SNMP, RMON, Telnet

Tecnología de conectividad: Cableado

Modo comunicación: Semidúplex, dúplex pleno

Protocolo de conmutación: Ethernet

Tamaño de tabla de dirección MAC: 8K de entradas

Indicadores de estado: Estado puerto, actividad de enlace, estado de colisión, velocidad de transmisión del puerto, modo puerto duplex, ancho de banda utilización %, alimentación.

Monitorización en red, capacidad duplex, enlace ascendente, soporte VLAN, activable, apilable.

Alimentación

Dispositivo de alimentación: Fuente de alimentación - interna

Voltaje necesario: CA 120/230 V (50/60 Hz)

Consumo eléctrico en funcionamiento: 45 vatios.

2. **Router Cisco SOHO 91:**

Memoria

Memoria RAM: 64 MB (instalados) / 64 MB (máx.)

Memoria Flash: 8 MB (instalados) / 8 MB (máx.)

Conexión de redes

Tecnologia de conectividad: Cableado

Protocolo de interconexión de datos: Ethernet, Fast Ethernet

Protocolo de conmutación: Ethernet

Red / Protocolo de transporte: TCP/IP, PPTP, IPSec, PPPoE

Protocolo de direccionamiento: RIP-1, RIP-2

Protocolo de gestión remota: SNMP, Telnet, HTTP

Protección firewall, conmutación, Encaminamiento IP, soporte de DHCP, soporte de NAT, cifrado de 64 bits, conmutador MDI/MDI-X, VPN, soporte para PAT.

Alimentación

Dispositivo de alimentación: Adaptador de corriente - externo

Voltaje necesario: CA 100/240 V (50/60 Hz)

Consumo eléctrico en funcionamiento: 10 vatios

3. **UPS Blazer 2000 Regulada:**

Controlada por microprocesador.
Equipada con regulador automático de voltaje, función DC para encenderlo sin necesidad de corriente AC.
Puerto de Comunicación RS-232.
Función de ahorro de energía, apaga la UPS cuando no hay carga.
Carga la batería cuando esta en OFF.
Compacto y liviano Filtro protector de Modem/Internet, protegido contra sobrecargas.
Regulador de Voltaje Incorporado.
Software para Windows 95/98/NT/2000/ME/XP, Novell y Linux.
Visualiza Voltajes, carga del UPS, carga de bateria, frecuencia.
Graba sus archivos y apaga su PC automáticamente.

4. **Servidor para Rack Dell PowerEdge:**

Procesador: De secuencia 5100 con hasta dos buses frontales a 3 GHz, 1066 MHz o 1333 MHz y 4 MB de caché de nivel 2.

Memoria: DIMM en búfer con ECC de hasta 32 GB.

Almacenamiento: SAS de 3,5 pulgadas (a 10.000 rpm): discos duros de 73 GB, 146 GB, 300 GB en caliente.

Opciones de copia de seguridad en cinta.

Opciones de almacenamiento externo.

3 opciones básicas de disco duro:

- Opción de 4 discos duros

4 unidades x SAS de 3,5 pulgadas (a 10.000/15.000 rpm) o SATA (7200)

Compartimentos para periféricos: 1 compartimento delgado para unidad de disquete opcional, con opción de CD-ROM, DVD-ROM o unidad combinada de CD-RW/DVD-ROM

Alimentación: Fuente de alimentación redundante opcional conectable en marcha de 750 vatios, 110/220 voltios

Dispositivos de Entrada:

- Ratón Dell USB
- Teclado Dell USB
- Unidad de memoria Flash USB de 128 MB o 256 MB
- Unidad de disquete USB externa

5. Rack HP Shock Pallet

Tamaño: 19"

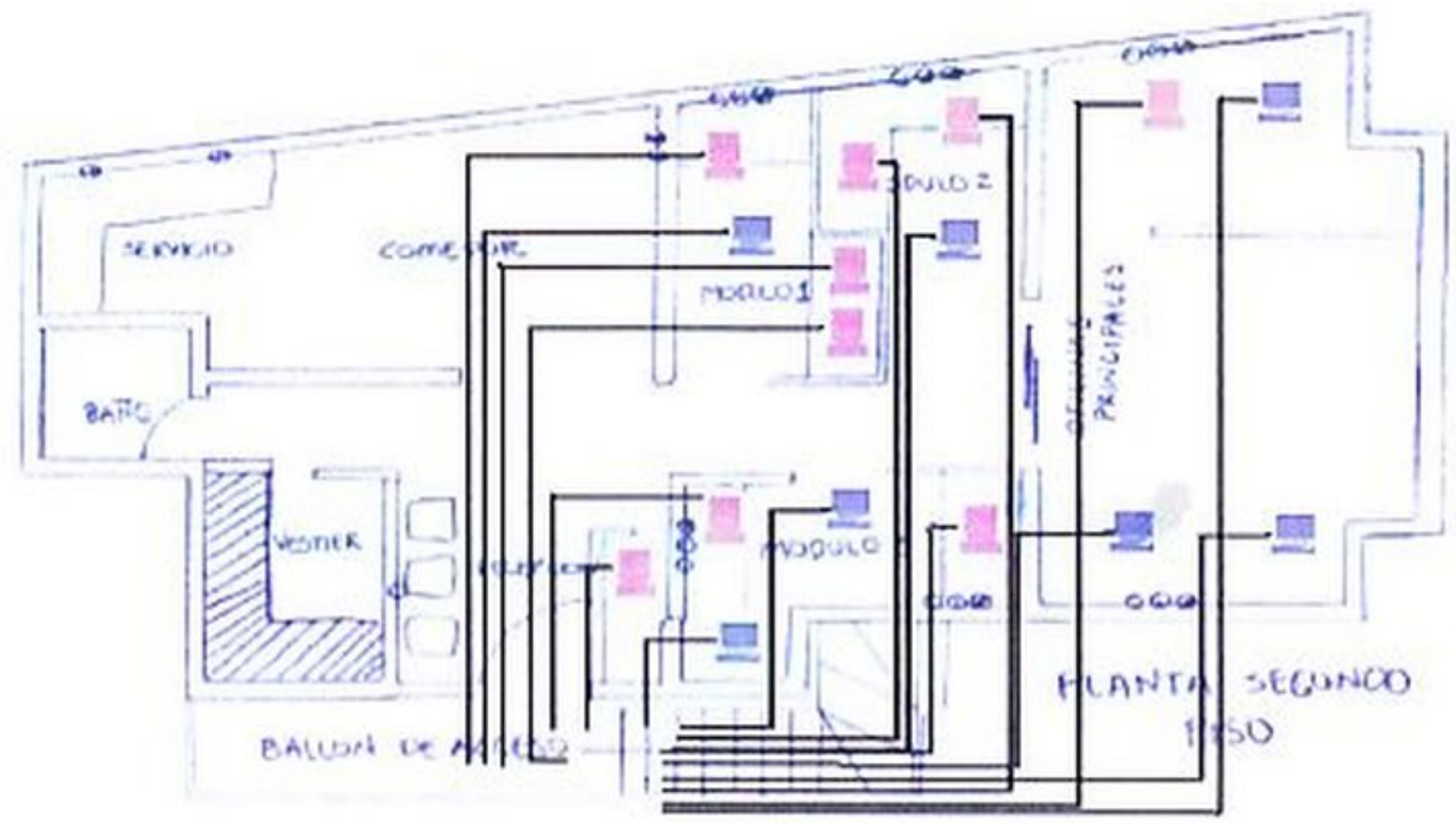
Altura (unidades de bastidor): 42 U

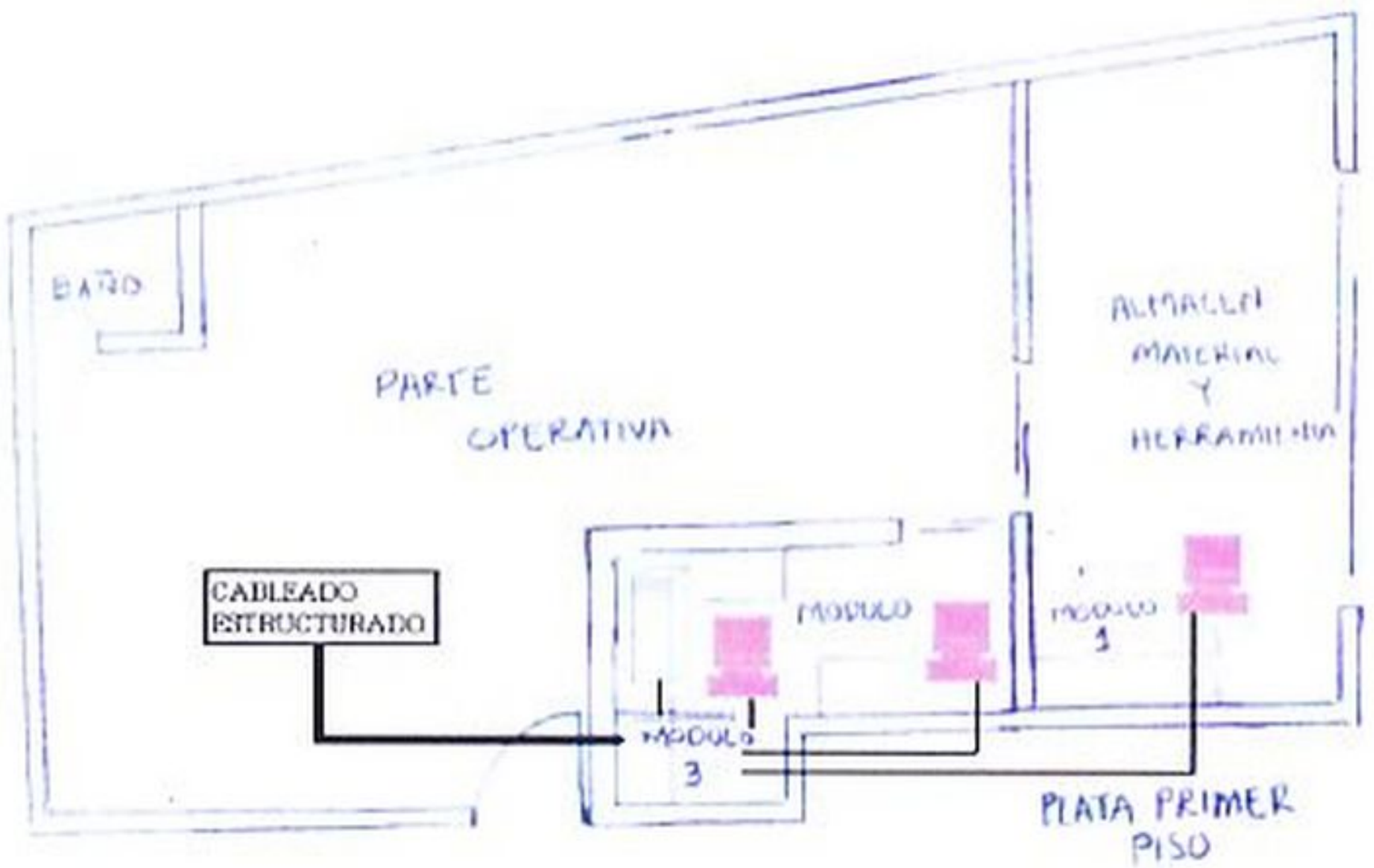
Material del producto: Metal

Dimensiones (Ancho x Profundidad x Altura): 61 cm x 101 cm x 200 cm

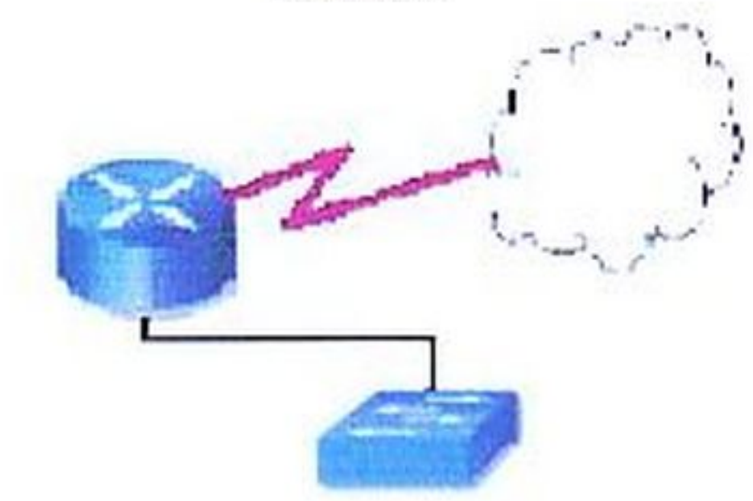
Peso: 114.8 kg

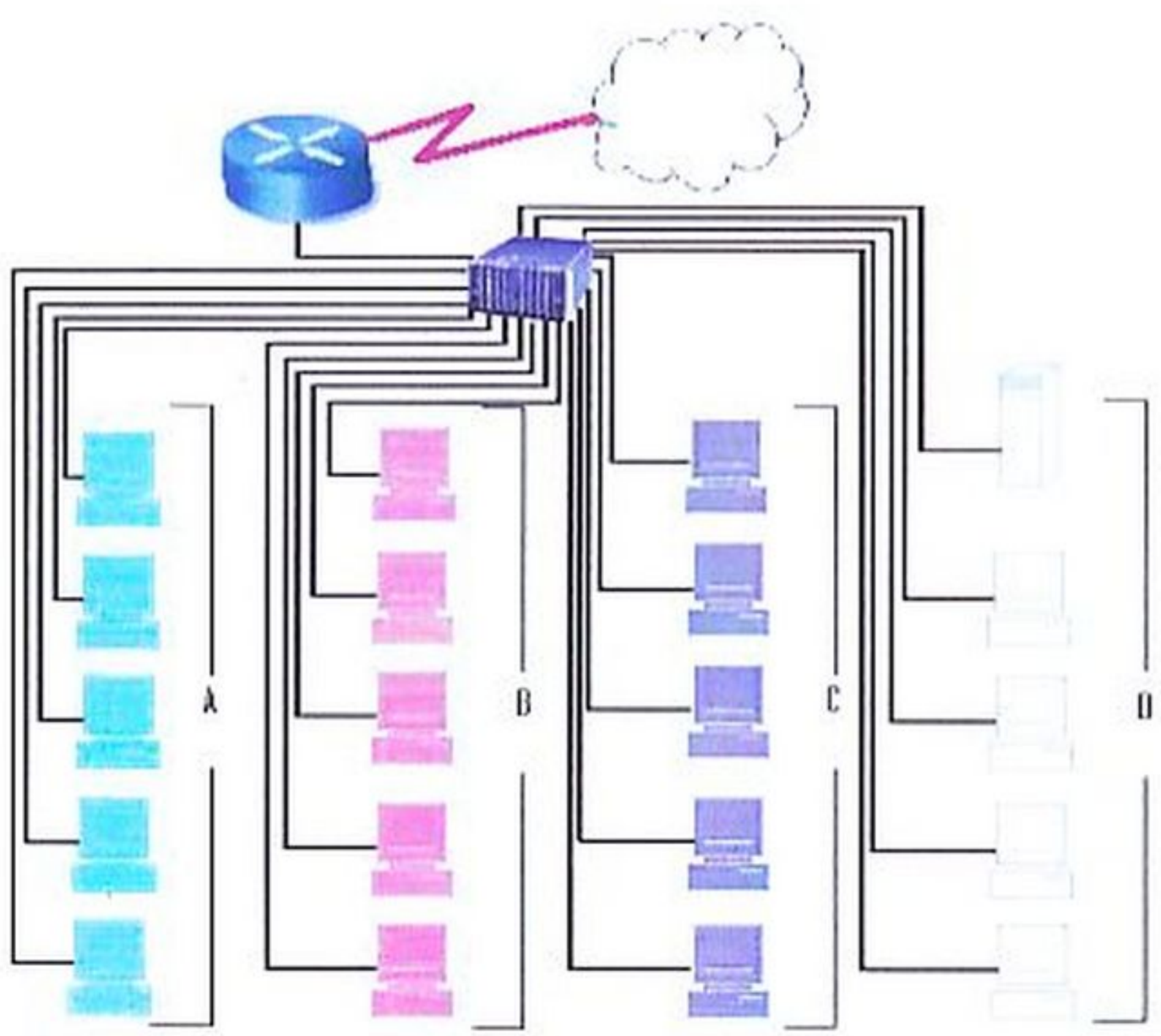
14.2 MAPA LOGICO PROPUESTO





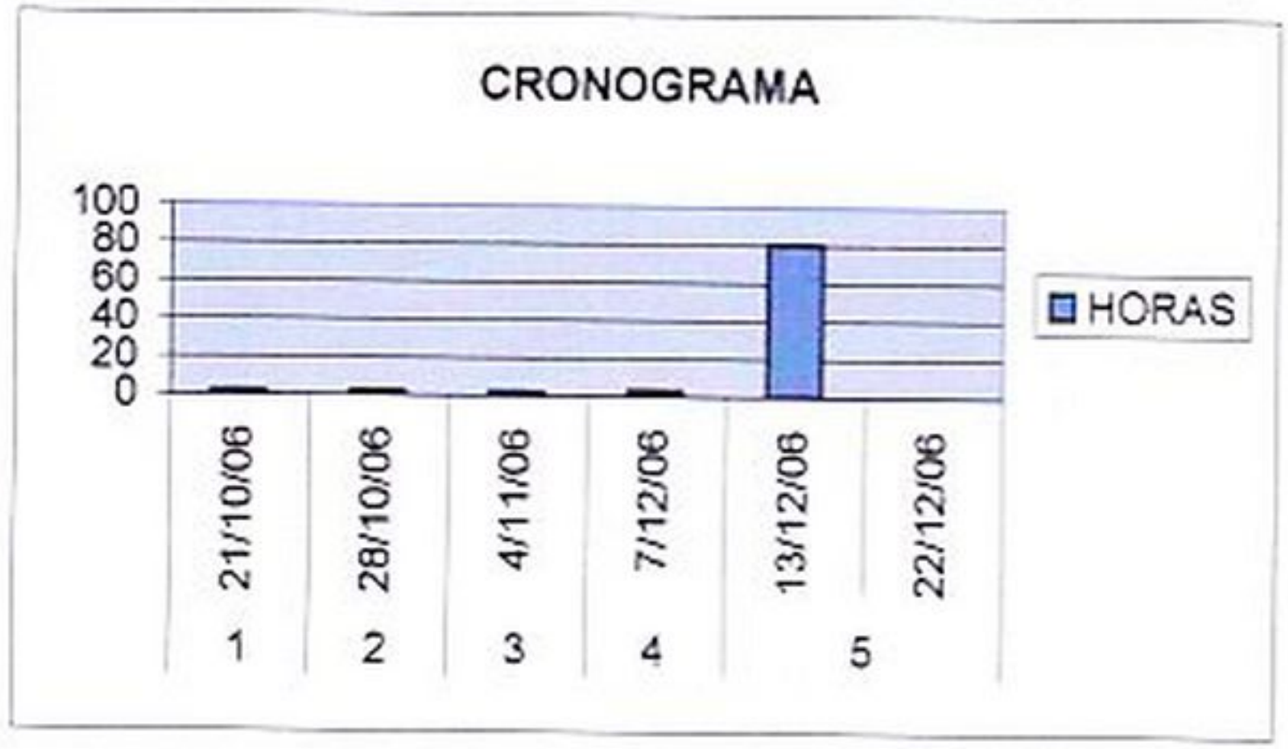
MODULO





CRONOGRAMA		
ACTIVIDAD	FECHAS	HORAS
1	21/10/06	2
2	28/10/06	2
3	4/11/06	2
4	7/12/06	3
5	13/12/06 22/12/06	80

CONVENCIONES	
1	Reunión con la Subgerente Graciela Cortés
2	Visita a la sede Metaliza
3	Presentación de la Propuesta
4	Aprobación de Proyecto
5	Desarrollo del Proyecto



COSTOS			
Material	**Cantidad**	**Valor Unitario**	**Valor Total**
Canaleta por Tramos	25	$ 27.000,00	$ 675.000,00
Escalerilla por Tramos	8	$ 48.000,00	$ 384.000,00
Cable por metro Categoria 6	300	$ 1.000,00	$ 300.000,00
Cable de Corriente por metro	70	$ 1.500,00	$ 105.000,00
Toma de Red	24	$ 3.200,00	$ 76.800,00
Toma del Cable	24	$ 2.700,00	$ 64.800,00
Conector RJ 45	100	$ 800,00	$ 80.000,00
Equipos			
Rack HP Shock Pallet	1	$ 4.182.158,00	$ 4.182.158,00
Router Cisco SOHO 91	1	$ 689.811,00	$ 689.811,00
Switch Catalyst_24P	1	$ 300.000,00	$ 300.000,00
Servidor para Rack Dell PowerEdge	1	$ 4.830.000,00	$ 4.830.000,00
UPS Blazer 2000 Regulada	1	$ 735.000,00	$ 735.000,00
Mano de Obra x Dia	25	$ 90.000,00	$ 2.250.000,00
Mano de Obra Civil			$ 500.000,00
Diseño de la Red			$ 2.000.000,00

Total		**$ 17.172.569,00**

CONCLUSIONES

1. Con el desarrollo del proyecto, se logró optimizar los conocimientos adquiridos a través del curso.
2. Para llevar a cabo el proyecto, se tuvieron en cuenta los siguientes aspectos: organizacional, tecnológico y financiero; mediante los cuales se pudo concretar la propuesta presentada a la empresa.
3. Es importante resaltar, que para la ejecución de cualquier proyecto es indispensable el trabajo en equipo, la distribución de tareas y la asignación de responsabilidades, ya que de esta manera se complementa la labor requerida.

BIBLIOGRAFIA

- CISCO SYSTEMS, INC. ACADEMIA DE NETWORKING DE CISCO SYSTEMS. GUIA DEL PRIMER AÑO CCNA 1 Y 2. Pearson Educación S.A.. 2004
- CISCO SYSTEMS, INC. ACADEMIA DE NETWORKING DE CISCO SYSTEMS. GUIA DEL SEGUNDO AÑO CCNA 3 Y 4. Pearson Educación S.A.. 2004
- www.google.com