UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

CAMPUS
A R A G O N

"CONECTIVIDAD, ADMINISTRACION Y MONITOREO DE CENTROS DE CONTROL"

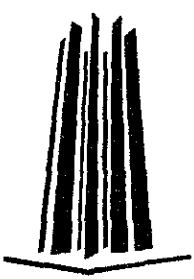
TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A

FRANCISCO JAVIER RIVERA PEREZ



ENEP ARAGON

MEXICO. 1998

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

La presente Tesis la dedico a mis Padres:

Marcial Rivera Olvera

Ricarda Pèrez Sánchez

Por darme la vida, educación y mucho cariño. Por que sin ella no sería posible mi realización como hombre y profesionista

Gracias por todo

A mis hermanos Angel, Mireya, Monica, Tíos y Familia

Por el amor que me tienen y por contar siempre con ellos.

Gracias.

A Mis Amigos:

Miriam Mialma y Lino González

Adolfo Rodríguez Acosta

Eduardo Navarrete y familia

Alejandro Bermúdez y Familia

Elena Ramírez Rangel y Familia

Amigos del Centro de Computo Aragon

Y a todos ellos que en su momento me Apoyaron con sus Consejos y Amistad.

Gracias.

CONECTIVIDAD, ADMINISTRACION Y MONITOREO DE CENTROS DE CONTROL.

INDICE

INTRODUCCION.

Es importante el administrar y tener el control de una pequeña o mediana red LAN, pero se vuelve un tanto más complicado el tratar de administrar una red que se forma de varias redes LAN, es por ello que es necesario un centro de control, ya que no tan solo es una red de redes LAN, sino que la conforman otras tres tipos de redes X.25, LAN, TCPIP y SNA.

Se podía considerar en un tiempo 80's que era casi imposible el tratar de interconectar redes LAN con ambientes de Redes Mainframe esto es la convivencia de múltiples protocolos como el IPX de novel o el TCP/IP para ambientes UNIX. Y más aun el tratar de conectar una Red SNA.

Esto es gracias a que las compañías tratan de seguir el modelo OSI para tratar de inter conectar sus equipos tratando de seguir este modelo, así como de los sistemas operativos.

Y compañías que se dedican a desarrollar nuevas tecnologías para interconectar equipos de comunicación con manejo de muntiples protocolos

y compañías que desarrollan software para administrar o bien tratar de que sean mas amigables los ambientes operativos que por años han sido complicados aun para los que trabajan en este medio de las comunicaciones y la computación

el propósito de la presente tesis es el tratar de dar una visión general de las redes que interactuan en una compañía de comunicaciones y la forma en como se resolvieron algunas de sus principales problemas de comunicación. Aunado a la implementación de nueva tecnología así como la implementación de nuevas metodologías para la resolución de problemas.

ADMINISTRACION Y MONITOREO DE REDES

Las redes LAN, MAN ya no son islas individuales de tecnología. Originalmente se instalaban y administraban por separado con el fin de dirigir las necesidades de las diferentes organizaciones, sin embargo ahora se están interconectando para crear organizaciones cada vez mayores, redes corporativas que le dan soporte a la misión crítica. El buscar soluciones para poder administrar esta disímil colección de equipos se ha convertido en uno de los temas más comunes de la tecnología actual. La administración de redes es un tema muy vasto que cubre un amplio rango de actividades por lo que muchas veces se considera extremadamente confuso.

¿Que es La administración de redes?. Es un término cerrado. Es la sombrilla bajo la cual una gran variedad de productos, desde un cable, hardware(equipo de comunicaciones) hasta el mejor software, se pueden clasificar, monitorear y corregir. No hay punto de discusión en que la principal tarea de la administración de la red es la emisión de mensajes de alerta para el administrador conforme surgen problemas. Estas alarmas le permitirán al administrador

mantener la red corriendo y maximizar su aprovechamiento para ofrecer buenos tiempos de respuesta.

A pesar de que las redes hoy en día consisten de múltiples tecnologías y equipos de diferentes proveedores, el reto es poder manejarlas como una unidad.

Es necesario adoptar un marco de trabajo que esté estandarizado para la administración de redes.

Una posible definición para conseguir esta meta la Organización Internacional de Standards (ISO) ha categorizado las funciones de la administración de redes en dministración de fallas, Administración de funcionamiento, Administración de configuración, Administración de cuentas, Administración de seguridad.

ANTECEDENTES

Los sistemas operativos de red local, aportan soluciones para compartir información y recursos locales. Los mainframes, proveen soluciones para el procesamiento de grandes volúmenes de información. Es utópico pensar, que una red local realice esta tarea, con la eficiencia de un Mainframe. De igual manera, un Mainframe no ejecuta el trabajo de una red LAN. Cada cual satisface una necesidad diferente y se complementa para ofrecer una solución integral a las empresas.

Como se complementan ambas plataformas

Conectividad. Un Gateway (puente de comunicación) es la solución para compartir información o recursos remotos (Mainframe, servicios de información, bases de datos, otras redes locales) las cuales crean una red amplia (WAN) en el proceso. La interconexión interconexión es por lo general es transparente para el usuario final, lo cual permite que la información fluya con seguridad y libremente por una RED WAN.

El administrar este tipo de red Wan es un tanto complicado si no se tienen algunas consideraciones debido a que una red WAN esta formada por diferentes arquitecturas y plataformas así como diferentes tipos de protocolos es necesario estandarizar estos sistemas en lo más posible.

El tratar de monitorear una red plana en la que solo se sabe que tiene una identificación (LU) unidad lógica o un a dirección IP, sin saber donde se encuentra ubicada es un tanto difícil tratar de dar soporte sin que el personal que tiene mayor experiencia o sabe como se encuentra estructurada la red este presente.

bien el tratar de monitorear la red en cada uno de los ambientes operativos, ejemplo de esto es monitorear una red TCP/IP y conocer sobre Cisco Works . o NetView para MVS y dar solución a los problemas de este tipo de red aun más tratar de dar solución a los problemas de usuarios de redes Lan Novell es un tanto complicado.

Es por ello que el presente documento pretende dar una visión de como se debe implementar un centro de control con las herramientas necesarias para que el administrador que se encargue del monitoreo tenga una base bien definida de los problemas y como solucionarlos antes de estos se presenten. utilizando herramientas de monitoreo así como dispositivos de diagnostico y análisis de protocolos etc.

Así como administrar de una mejor manera los recursos humanos y reducir las cuestiones administrativas.

CAPITULO I. CONCEPTOS Y ELEMENTOS NECESARIOS PARA CONECTAR E INTERCONECTAR REDES.

I.1. INTRODUCCIÓN A LAS REDES COMPUTACIONALES

En el presente capitulo se propone integrar una serie de conocimientos que son fundamentales para la comprensión de los capítulos Subsecuentes como Que es una red, Modelos existen actualmente, Tipos de redes que existen, Servicios que proporciona una RED, Medios de transmisión más comunes, Conexión al medio de transmisión, Modelos y protocolos de red, Modelo OSI y Sistemas operativos:

Que es una red; donde se hablara de los modelos (centralizado, distribuido y colaborativo)

Tipos de redes que existen; donde se hablara des redes LAN, MAN, WAN y las Enterprice y Global

Elementos necesarios para una red; donde se describiran los elementos necesarios para una red como son (servicios que ofrece una red, medio de trasmisión, Conexión al medio y las reglas de comunicación o Protocolo), así como Modelos y protocolos de red, Modelo OSI y sistemas operativos.

I.1.1. ¿QUE ES UNA RED?

El concepto fundamental de una red es compartir información y recursos así como servicios. Las redes de computación proveen las herramientas de comunicación para permitir a otras computadoras compartir información y habilidades.

Hoy en día se han desarrollado nuevas tecnologías de redes computacionales, denominados Modelos Computacionales, de los cuales sobresalen los siguientes:

Modelo Centralizado:

Modelo Distribuido:

Modelo Colaborativo: Es un nuevo modelo también llamado (called cooperative processing), en el cual se comparte la carga de trabajo entre dos o mas computadoras, tales como una macro computadora y una computadora personal, esto implica dividir la carga de trabajo mas eficientemente, este modelo es similar al distribuido.

I.1.2. LAS REDES DE HOY EN DÍA.

Las redes de hoy en día incluyen un gran numero de computadoras y sistemas operativos para computadoras asociados con los 3 modelos antes mencionados, una red típica incluye Mainframes, computadoras personales y una gran variedad de dispositivos de comunicaciones como Gateways, Ruteadores, Concentradores etc. Estas redes pueden ser clasificadas por su tamaño, la distancia que cubren o el tipo de estructura que forman. La denominación que a estas se les da es la siguiente:

Redes de Area Local	**LAN**	Local Area Network
Redes de Area Metropolitana	**MAN**	Metropolitan Area Network
Redes de Area Amplia	**WAN**	Wide Area Network

Redes de Area Local(LAN): Una red de área Local se refiere a la combinación de Hardware (computadoras) y el medio de transmisión son relativamente pequeños. Las redes LAN Generalmente no exceden más de 10 por kilometro y solo utilizan un medio de transmisión.

Redes de Area Metropolitana (MAN): Es un tipo de red un poco más grande que una red LAN, es llamada metropolitana en el momento en que cubre una ciudad (1000KMs.).

Redes de Area Amplia WAN: son aquellas redes que incluyen gran parte de redes MAN y LAN al rededor del mundo.

Dentro de las WAN se han designado dos categorías nuevas (Enterprice y la Global), la Interprice esta definida como la interconexión de varias red LAN de una misma organización y la Global a diferencia de la interprice es que pude tener cobertura mundial pero además involucrar varias organizaciones.

I.1.3. ELEMENTOS QUE SE REQUIEREN PARA UNA RED.

Todas las redes requieren de los siguientes tres elementos básicos:

1.- Tener al menos 2 individuos quienes tienen que compartir algo
2.- Tener un método o una ruta(pathway) para contactar cada uno.
3.- Tener reglas para que estos dos o más individuos puedan comunicarse.

Para entender lo anterior supongamos la siguiente analogía relacionando la comunicación humana con una red

Suponiendo que usted es un científico y que esta trabajando sobre determinado tema científico y usted se entera de que hay otro científico en algún lugar de Europa que también esta trabajando en el mismo tema y usted desea pedirle información, esto sería el primer

requerimiento (Compartir). Ahora suponiendo que usted no sabe como comenzar (contactar), usted primero debe escribir una carta y enviarla pero para poder enviarla usted requiere de del servicio postal para contactar a otra persona. Esto vendría siendo el segundo requerimiento

Ahora bien aunque su carta halla sido recibida, esto no implica que allá sido comprendida por el otro científico, para comprenderla este ultimo tendrá que solicitar los servicios de una persona que entienda el idioma en el cual usted le escribió reglas (protocolo).

En términos generales una red es simplemente la compartición de recurso, servicios e información.

I.2. SERVICIOS QUE PROPORCIONA UNA RED.

En esta sección se pretende definir los primeros elementos básicos de una red de computadoras, así como identificar y describir cada una de las funciones de servidor de archivos, Servidores de impresión, Servidor de bases de datos, Servicios de mensajería y Servicios de aplicación.

Cabe señalar que todos estos servicios actúan en la ultima capa del modelo OSI (capa de aplicación).

Las aplicaciones para computadoras requieren de una combinación de Datos, Poder de procesamiento y recursos de Entrada /salida para acoplamiento de tareas. Los servicios de una red permiten utilizar sus recursos requiriendo de una aplicación de red especial.

Los sistemas operativos (OS/2, DOS, Open VMS y UNIX) son una serie de programas que manejan los recursos de las computadoras como son (CPU, Memoria, periféricos etc.), a diferencia de un sistema operativo que reside en una simple computadora, los sistemas operativos de red (NOS) pueden ser distribuidos sobre algunas computadoras de una red.

Cuando se elija un sistema operativo se debe tener énfasis o atención en cuales son los servicios que usted necesita y cuales son los servicios que este ofrece, a continuación se mencionan los servicios más importantes que se debe tener un sistema operativo de red:

I.2.1. SERVICIOS DE ARCHIVOS (FILE SERVICES).

Los servicios de archivo Incluyen aplicaciones de red diseñadas a eficientar el almacenamiento y recuperación de archivos o mover archivos de datos. Además de aumentar el rendimiento en lectura, escritura, control de acceso y la manipulación de los datos. Los beneficios que nos puede traer estos es que se pueden mover mas rápidamente los archivos

de un lugar a otro, utilizar eficientemente los dispositivos de almacenamiento, manejas multiples copias del mismo archivo y realizar respaldos de archivos de datos criticos.

- Transferencia de archivos (File Transfer)
- Almacenamiento de datos y Migración de archivos
- Archivación de archivos

I.2.2. SERVICIOS DE IMPRESIÓN (PRINT SEVICES).

Los servicios de impresión son aplicaciones de red que manejan el acceso y control de impresoras y Fax. Los servicios de impresión aceptan tareas e interpretan formatos de impresión y manejar colas de impresión. Los beneficios que proporcionan son:

- Reducen el numero de impresoras que una compañía necesita
- Colocar sitios de impresión donde son más convenientes
- Las colas de impresión reducen el tiempo en que una computadora espera respuesta cuando envía un trabajo e impresión.
- Permiten compartir eficientemente las impresoras
- Permiten también computarizar la transmisión y recepción de imágenes de Fax.

I.2.3. SERVICIOS DE BASES DE DATOS (DATABASE SERVICES).

Los servicios de bases de datos proveen a una base de datos de datos o información permitiéndole a un usuario almacenar, recuperar y tener control sobre una base de datos, Un termino especial a sido creado para describir las aplicaciones de bases de datos, el termino es llamado Cliente-Servidor Database.

Los servicios de bases de datos optiman en las computadoras el almacenamiento, la ordenación, las búsquedas y la recuperación de registros, provee seguridad en los datos, reduce el tiempo de respuesta incrementando el numero de transacciones por segundo y como consecuencia reduce el trafico en una red.

I.2.4. SERVICIOS DE MENSAJERÍA (MESSAGE SERVICES).

Los servicios de mensajería incluyen almacenamiento, acceso y manejo de archivos tipo texto, binario, gráficos, vídeo y audio, los servicios de mensajes son similares a los servicios de archivos. Un servicio de mensajes similar al file server, la cual permite servicios de Datos, voz, vídeo.

Servicios de Aplicaciones (Application Services)

I.3. MEDIOS DE TRANSMISIÓN MÁS COMUNES.

Esta sección se pretende dar una revisión a los segundos elementos básicos de una red, a estos segundos elementos se clasifica como medio de transmisión, así como su definición e identificar los diferentes medios de transmisión más comunes. A demás de las características de cada uno, incluyendo: su costo, su facilidad de instalación, su capacidad, atenuación e inmunidad a la interferencia de señales.

I.3.1. MEDIO DE TRANSMISIÓN EN REDES.

Para que los servicios y recursos de una red puedan ser compartidos, la Red de computadoras debe tener una ruta de conexión para contactar una u otras computadoras, la ruta sobre la cual se puedan enviar pulsos de corriente eléctrica, microondas o algún tipo de energía clasificado dentro del espectro electromagnético. Para transmitir señales. Se le denomina medio de transmisión.

En otras palabras tipo de conexión puede ser físico (conductor) o bien inalámbrico (espectro electromagnético) para transmitir o recibir información.

Ya que sobre este tipo de medio se pueden representar dos estados (binario) unos y ceros., este tipo de señalización es el que utilizan las computadoras hoy en día para comunicarse.

A continuación se describen los diferentes medios de transmisión más comunes, comparando sus principales características, sus posibles beneficios y tomando algunas consideraciones como lo son (costo, fácil instalación, Atenuación e inmunidad a la interferencia electromagnética (EMI).

Medio Cableado

El medio cableado se encuentra dividido por Par trenzado, coaxial y fibra óptica, que requieren de un medio físico (cobre o vidrio) para transmitir información, Ethernet estándar 802.3 de IEEE originalmente creada y desarrollada por Xerox, y posteriormente por Digital e Intel que utiliza el método de acceso CSMA/CD, transmite a 10Mbps y puede conectar en total hasta 1.024 nodos.

Par trenzado

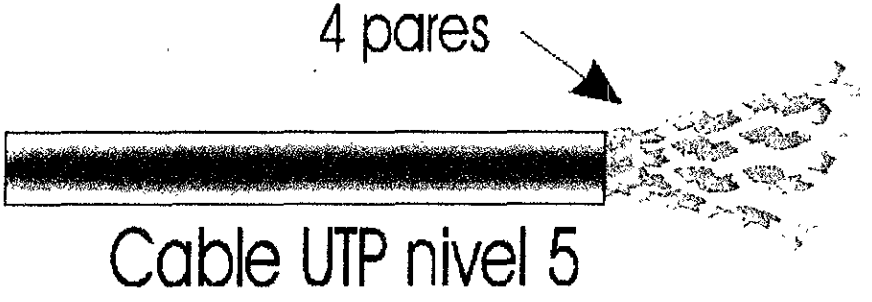
Normalizado por la IEEE y que hace referencia al tipo de envío de paquetes a través de las redes de área local 802.3 (Ethernet) de 10Mbps, también llamada 10baseT que operan con pares de cables trenzados no recubiertos, en lugar de cable coaxial por un medio físico y que

esta formado por un par de pequeños alambres aislados que se emplean comúnmente en los cables telefónicos. Los alambres se encuentran retorcidos uno alrededor del otro a fin de minimizar la interferencia proveniente de otros alambres. Los cables de par trenzado tienen un ancho de banda limitado en comparación con los del tipo coaxiales y la fibra óptica La norma 10 base T también indica que no es recomendable utilizar este medio para cubrir grandes distancias para interconectar Redes ya que solo puede tener una cobertura no mayor a 100 metros, sin la necesidad de conectar un repetidor. Adicionalmente se puede decir que forman un total de 4 pares y que están codificados por colores. Existen 2 tipos de cables trenzados que a continuación se describen:

UTP

(Unshield Twister Pair) También llamado par trenzado sin blindaje, el cual es uno de los más utilizados en telefonía y transmisión de datos ya que es más económico que el de tipo Coaxial, Además se puede instalar con diferentes configuraciones. Según la IEA quien es la organización que norma y pone reglas en cuanto a la calidad de los tipos de cable, menciona que hay diferentes tipos de cables y que estos se clasifican por niveles, los más comunes son el cable de nivel 3 y nivel 5.

Por ser barato es utilizado en sistemas de telefonía y en equipo o dispositivo hacia paneles de líneas pasando por centrales telefónicas y después pasar por un patch panel y siguiendo con el mismo tipo de cable hacia otros dispositivos comunes en las redes como HUB´S, RUTEADORES y GATEWAY con algún tipo de Transductor, como se puede observar es un cable que puede ser utilizado para uso general. Incluso para transmisiones de Voz.

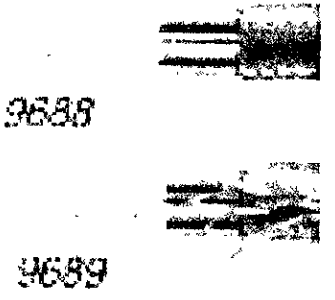


STP

(Shiel Twister Pair) o Par Trenzado Protegido es un tipo de cable similar al UTP, utilizado comúnmente en Tendidos telefónicos, el cual se encuentra envuelto por una cubierta metálica para eliminar interferencias externas, que pueden provocar inducción de ruido en las señales de voz y datos.

Nota: Cabe señalar que se han relizado pruebas con de proximidad de cable UTP/STP a Balastras de iluminación fluorescente sin presentar alguna distorsión en las señales.

La colocación de los cables UTP en estrecha proximidad a los dispositivos de alumbrado fluorescente y el ciclo rápido de la energía del dispositivo de alumbrado representa un caso extremo de ruido del dispositivo. Con el ciclo rápido de la energía, la teoría es que la energía transitoria, que se crea a partir del reactor y del interruptor, se incrementa substancialmente en el dispositivo. Este ruido eléctrico puede volverse muy destructivo para los datos en cables de comunicación colocados en estrecha proximidad a los dispositivos. Se demostró que incluso bajo estas condiciones extremas, no se observó error alguno. Considerando estos datos, se ha determinado que los cables UTP no requieren separación al colocarse directamente arriba de o adyacentes a los dispositivos de alumbrado fluorescente.



Cable Par Trenzado 1

Coaxial

Este tipo de medio está formado por un centro delgado de cobre, cubierto por una capa plástica que lo protege, el cual transmite las señales digitales; sobre la misma cubierta se encuentra otro conductor trenzado y por ultimo una cubierta que cubre a ambos conductores.

Es un cable de alta capacidad utilizado en voz, vídeo y datos generalmente llamado co-ax. Contiene un alambre aislado, sólido o multifilamento, que está rodeado por una pantalla sólida o de malla trenzada, bajo una cubierta exterior. Un revestimiento exterior de teflón para protección contra incendios, es opcional. A pesar de la similitud de apariencias, existen múltiples tipos de cable coaxial, cada uno con un diámetro y una impedancia diferentes para un propósito definido (TV, banda base, banda ancha). Los cables coaxiales proveen un ancho de banda muy superior al de los de tipo par trenzados.

Coaxial Grueso 1

Coaxial Delgado 1

Fibra Optica

La fibra óptica es otro cable (a base de vidrio protegido por una cubierta plástica) que es utilizado como medio de transmisión, este tipo de fibra se le encuentra en dos presentaciones (mono-modo y multi-modo); la principal diferencia entre estos dos tipos de fibra, su funcionamiento esta basado en la transmisión de impulsos luminosos a través de la fibra además de utilizar Diodos transductores (LED, ILDs) para convertir los impulsos luminosos en variaciones de corriente; que son utilizados por las computadoras de hoy en día para representar valores binarios (ceros y unos).

El **Conector SC** cuenta con una armazón moldeada y sistema de cerrado a presión. Perfecto para la oficina, televisión de cable CATV y aplicaciones telefónicas.

EL **Conector ST**® utiliza un sistema de cerrado de bayoneta. Su férula de cerámica le asegura un alta eficiencia.

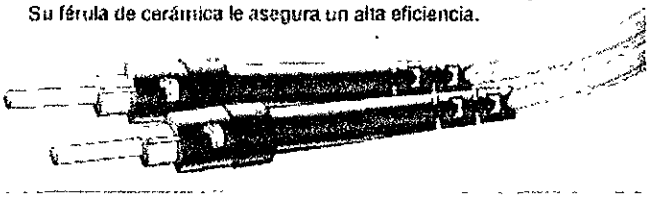


Tabla Comparativa

Medio Alambrico	*TP*		*Coaxial*		*Fibra Optica*	
	UTP	*STP*	*Delgado*	*Grueso*	*Modal*	*Multimodal*
Norma	10 Base T	10 Base T	10 Base 2	10 Base 5	10 Base F	10 Base F
Topología	Ethernet BUS	Ethernet BUS	Ethernet BUS	Ethernet BUS	Ethe/token Ring	Ethe/token Ring
Distancia Max.	<100 mts.	<100mts	<200 mts	<500 mts.	100gbps>2gbps	100gbps>2gbps
Capacidad						
Instalación	Fácil	Fácil	med. Fácil	med. Fácil	Difícil, ya que se requiere de equipo especial para ello.	Difícil, ya que se requiere de equipo especial para ello.
Atenuación					ninguna	ninguna
Inmunidad IME	muy poca	Blindado	Blindado	Blindado	Nula, ya que usa señales luminosas	Nula, ya que usa señales luminosas
Costo	Bajo <Coaxial	Bajo<Coaxial	Bajo<Fibra O.	Bajo<Fibra O	Caro	Caro

I.3.2. MEDIO INALÁMBRICO.

Otra forma de transmitir información es el utilizando el medio inalámbrico, esto es enviar datos sin la utilización de algún tipo de cable o conductor físico, este medio generalmente utiliza señales electromagnéticas, existen básicamente 3 tipos de medios inalámbricos *Radio frecuencia, Micro Ondas y Ondas de luz Infrarrojo,* el nombre que seles a asignado por convención es para dividir parte del espectro electromagnético según el rango de frecuencia que le fue asignado. El implementar este tipo de medio inalámbrico en la instalación de redes LAN y WAN requieren de una inversión Mayor. Obviamente es utilizado por compañías de comunicaciones que ofrecen y rentan el servicio.

A continuación se describe brevemente en que consiste cada tipo de onda:

Radio frecuencia

Todas las transmisiones radiales, desde las de radio AM hasta las de satélites, entran en este rango, que va desde los 30 KHz. hasta los 300 GHz. Es además un Sistema de identificación que utiliza etiquetas que transmiten un mensaje sin cable. y el rango de frecuencias

electromagnéticas es superior al de audio e inferior al de la luz visible. También se incluyen las ondas de TV y de radio FM en el rango de VHF(very high Frecuency) y (UHF) las de ultra alta frecuencia

Estas frecuencias también se pueden clasificar en **regulares** y **no regulares** esto que las personas que utilicen el algún rango del espectro electromagnético para transmitir señales deberán contar con el permiso de alguna institución que norme o asigne rangos dentro de la banda de radio frecuencia, Por el contrario si no se encuentran dentro de norma son personas irregulares que pueden con sus señales interferir en las que si se encuentran reguladas. En México la institución que regula y norma el medio de las comunicaciones es la SCT(secretaria de comunicaciones y transportes)

Para la transmisión y recepción de señales de radio, es necesario un dispositivo llamado antena, esta antena puede ser de los tipos siguientes, las de tipo Torre, Yagy, Dipolo y de antenas móviles, cada una de estas se utilizan para diferentes aplicaciones, pero clasifican general mente por la frecuencia que transmiten y la distancia que pueden cubrir. Entre más alto se encuentre una antena repetidora su recepción de la señal será mejor por ellos es recomendable utilizar satélites pare evitar el efecto de sombra, esto es cuando una antena transmisora emite una señal y se encuentra a baja altura, los receptores que se encuentran por detrás de algunas montañas estos no pueden recibir las señales.

Microondas

Las microondas son un tipo onda electromagnética similares a las de radio frecuencia excepto que varían entre 1 y 300 GHz o más. Las microondas son las frecuencias de transmisión frecuentemente utilizadas en sistemas de línea visual en la tierra así como también en satélites de comunicaciones.

Sistema Territorial

Línea de comunicaciones que viaja sobre, cerca o por debajo de la superficie terrestre. Este tipo de sistema es comúnmente utilizado en ciudades y en lugares accidentados o poco accesibles, para ello se requiere de la utilización de antenas parabólicas capaces de captar señales de alta frecuencia. Para que esto funcione se debe contar cuando menos dos antenas, viéndose una a la otra a esto se le denomina línea de vista. Este sistema es utilizado para conectar redes LAN de un edificio a otro o bien la distancia entre estos es varias cuadras.

Sistema Satelital

Este sistema de comunicaciones consta de una estación de conmutación de radio en órbita a 35.900 kilómetros sobre el ecuador llamado Satélite. El cual navega a la misma velocidad de rotación de la tierra (geoestacionario) de modo tal que pareciera que esta estacionado. Además contiene muchos canales de comunicaciones que reciben señales digitales y

analógicas de estaciones terrenas. Todas las señales son transmitidas en una frecuencia portadora La función de un satélite es amplificar y retransmitir las señales tierra, cubriendo o bien un área geográfica pequeña o bien casi una tercera parte de la superficie terrestre. Llegando aquellos sitios inaccesibles y también con esto se evita el efecto sombra. Además, los datos privados son a menudo cifrados como medida seguridad.

Ondas de luz Infrarrojo

Es otro tipo de medio inalámbrico basado en emisiones de luz infrarroja, y que utiliza diodos, diodos lasser y fotodiodos como dispositivos emisores de luz infrarroja, la utilización de este medio se ve mostrado prácticamente en algunos aparatos caseros y de oficina como controles remotos de televisores, equipos de sonido. La luz emitida por estos dispositivos es completamente pura, ya que únicamente contienen señales electromagnéticas, una desventaja de este tipo de sistema es que la luz infrarroja solo cubre distancias cortas y no es capaz de atravesar paredes o objetos opacos.

Existen dos grupos de clasificación de este tipo de tecnología ***Punto a punto*** y el ***Broadcast***, en el primer caso se requiere de un emisor y un solo receptor infrarrojo, mientras que en el segundo se necesita un emisor por varios receptores, actualmente este tipo de tecnología esta siendo utilizada por compañías como IBM, HP entre otras para implementar redes de computadoras. Básicamente en sus modelos de LAPTOP's las cuales ya tienen implementadas sensores infrarrojos para comunicarse y transferir información entre sí.

Una de las principales ventajas de utilizar este tipo de tecnología, es que no se requiere de tendido de cables para interconectar computadoras, utiliza un rango de frecuencia de de 100GHz. - 1000GHz. Es un tipo de tecnología medianamente barato. Se cree que este tipo de tecnología será utilizado a futuro. Una de sus principales desventajas es que aun no esta normado por completo. Existe una entidad que esta tratando de regular este tipo de tecnología IRDA(Infra Red Data Association).

I.4. CONEXION AL MEDIO DE TRASMISIÓN.

El medio de transmisión (cables) no es lo único que se requiere para la conexión de redes. Si no que existen otros dispositivos importantes. En esta sección se pretende identificar y describir la conexión física de computadoras e interconectarlas a un segmento sobre un medio de transmisión o incluso a varios tipos de redes, a través de los dispositivos más comúnmente utilizados así como el funcionamiento de los mismos.

Para lo anterior se puede clasificar en dos grupos de dispositivos de conexión, los cuales son denominados: Dispositivos de conexión de red (Network) y Dispositivos de interconexión de redes (Internetwork), del primer grupo se derivan los siguientes dispositivos (Conectores, Tarjetas, Módems, Repetidores, Hubs, Bridges y Multiplexores). Mientras que los del segundo grupo se clasifican en (Routers, Brouters y CSU/DSUs).

Los dispositivos de conexión de red se les clasifica así por que únicamente permiten conectar una o varias computadoras para formar una red, mientras que los dispositivos de interconexión de redes permiten conectar varios tipos de redes. Por lo cual es importante separarlos.

I.4.1. DISPOSITIVOS DE CONEXIÓN EN UNA RED.

Estos tipos de dispositivos permiten conectar a cada uno de los elementos (computadoras, Impresoras etc.) para formar un segmento de Red al medio de transmisión, a continuación se describen brevemente.

Conectores

Este tipo de dispositivo permite conectar a una computadora al medio de transmisión y actualmente existe en el mercado una gran variedad de conectores.

Si se quiere implementar una red bajo la norma Ethernet 802.3 de la IEEE es necesario, se puede implementar de utilizar algunos de los siguientes tipos de conectores.

Si se opta por cable coaxial delgado o grueso son necesarios conectores tipo BNC, conectores tipo T, y terminadores, que se colocan a los extremos del segmento.

Si se opta por cable tipo Par trenado, el más recomendado es el UTP(Unshield Twister Pair), serán necesarios conectores tipo RJ-45, este tipo de conectores son los mas utilizados.

Si se piensa implementar una red Token Ring serán necesarios conectores tipo DB-15, o bien V.35

Generalmente los conectores tipo DB9, DB25, y V.35 están enfocados a la transmisión tipo serial, de echo la V.35 se dice que es una versión mejorada de la norma.(RS-232).

Obviamente cada una de estos tipos de conectores están respaldadas por una serie de normas como lo son la 802.3 IEEE, la RS-232 etc. que indican las características y tipos de señalización en cada uno de estos conectores.

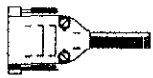
No necesariamente se tiene que seguir esta convención ya que también se pueden realizar nuevas configuraciones con estos mismos tipos de conectores. Por ejemplo se puede tener la configuración RS-232 tanto en un conector DB-9, DB-25 como en un V.35 incluso en un RJ-45, el detalle esta en saber identificar cada una de las señales. Como lo son Transmisión, recepción, señal de portadora etc.

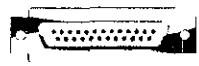
Accesorios Para cable coaxial, Unión o enpalme Coaxial, Conector Tipo "T", Conector BNC Coaxial, son algunos de los adaptadores y conectores utilizados en la instalación de cableado

de redes, en particular la de la norma 10base2 y la 10 base5 que señalan la implementación de redes LAN bajo Cable coaxial.

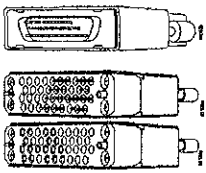

Conector DB9

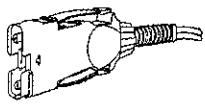

Conector Coaxial

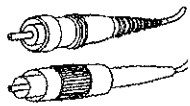

Concha DB25 o DB9

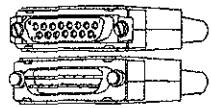

Conector DB25

Pero no son los únicos ya que existen algunos otros que son muy diversos y variados como los que a continuación se muestran, estos tipos de conectores son utilizados para la implementación de redes MAN y WAN, como es el caso de los conectores para fibra, V35 para dispositivos DTE o DCE o AUI.


Conector V35

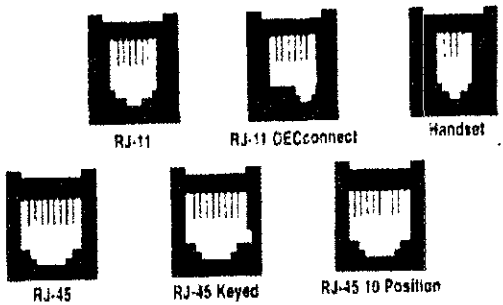

Conector para Fibra


Conector Fibra Optica


Conector AUI

Conector RJ

A continuación se muestra una serie de conectores RJ** que podemos encontrar en el mercado, cada uno es usado dependiendo del tipo de implementación de conexión.



Tarjetas

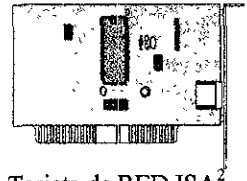
Actualmente existe una gran variedad de Tarjetas y transivers en el mercado. Las Tarjetas están formadas por una serie de circuitos impresos y mecanismos de conexión, necesarios para convertir las señales eléctricas que emite una estación de trabajo en impulsos eléctrico o señales electromagnéticas que permiten el intercambio de datos en una red, para ser usadas por el medio de transmisión. Este tipo de tarjetas generalmente no rebasan las dimensiones internas de una computadora ya que regularmente son colocadas en algún Puerto (SLOT) libre, también es necesario configurarla utilizando direcciones de memoria, así como asignarle una interrupción IRQ, las cuales no deben estar ocupadas por otro dispositivo ya que se generarían algún tipo de conflictos en la computadora. Cabe señalar que la configuración de tarjetas puede ser vía Hardware (intercambiando interruptores o jumpers) ó bien vía Software, para esto será necesario contar con los discos distribuidos por el proveedor o fabricante de las tarjetas para poder realizarlos. Así como definir el tipo del método de acceso (protocolo de enlace de datos), tales como Ethernet, Token Ring y LocalTalk. El medio de transmisión. generalmente este tipo de software tiene una presentación amigable, por lo que su instalación es muy sencilla.

Los transeivers al igual que las tarjetas esta conformadas por una serie componente electrónicos, que a su vez realizan la función de un transductor ya que pueden convertir los impulsos generados por la computadora en señales electromagnéticas o bien convertirlos impulsos luminosos para el caso de utilizar un medio de fibra óptica .incluso convertirlos en señales de luz infrarroja para el caso de una INFRARED.

De las tarjetas también se puede decir que tienen una identificación única que las hace diferentes entre si. Esto es desde que salen de fabrica tienen grabada esta información formada por nombre del fabricante y un número único, a esta identificación se le denomina MAC ADRESS.

Se puede decir que las tarjetas y los transivers son los dispositivos que permiten a las computadoras conectarse al medio físico.

Tarjeta De RED EISA[1]



Tarjeta de RED ISA[2]

Módems (MOdulator-DEModulator)

[1] *(Extended Industry Standard Architecture) arquitectura estándar industrial extendida Estándar de bus para PC que extiende la arquitectura del bus de la AT a 32 bits y permite a más de una CPU compartir el bus*

[2] *(Industry Standard Architecture) arquitectura industrial estándar Los buses de 8 bits (PC, XT), y de 16 bits (AT)*

MOdulador - DEModulador, Es un dispositivo que adapta una terminal o computadora a una línea telefónica. Convirtiendo los impulsos digitales de la computadora a frecuencias que se encuentran dentro del rango de audio, esto es para poder transmitirse a través de las líneas Telefónicas. Al otro extremo de la línea es necesario otro módem actuando como Demodulador, el cual convertir de nuevo en impulsos digitales para que sean entendidos por la computadora receptora.

El módem maneja el marcado y recepción de la llamada y controla la velocidad de transmisión. Los módems usados en líneas telefónicas transmiten a velocidades de 300, 1200, 2400, 4800, 9600 y 19200 byts por segundo. El régimen efectivo de datos es alrededor del 10% del régimen de bits; por lo tanto, 300 bps es equivalente a 30 caracteres por segundo. Llevaría un minuto completo llenar una pantalla a 300 bps; 15 segundos a 1200 bps y alrededor de 7 segundos a 2400 bps.

Usar un módem con una computadora personal requiere un puerto serial disponible para conectarlo, y un programa de comunicaciones.

Actualmente se están utilizando los módems para interconectar redes remotas, hoy en día la principal carrera en tecnología de fabricación de módems es crear uno que permita una gran capacidad de transferencia de datos. Por el momento se encuentran módems con tasas de transmisión del orden de los 14400 bps, 28.800 bps y los de 33.6 bps.

Existe un organo regulador llamado CCITT(Consultative Committee for International Telephony and Telegraphy), Comité Consultivo para telefonía y telegrafía Internacionales Una organización internacional de normas de comunicaciones. Es uno de los cuatro órganos de la Unión Internacional de Telecomunicaciones, fundada en 1865, con sede central en Ginebra y compuesta por más de 150 países miembros; Los módems Inteligentes están regidos por conjunto de ordenes (mandatos) AT Serie de instrucciones de máquina utilizadas para activar las capacidades de un módem. Desarrollado por Hayes Microcomputer Product, Inc., y formalmente llamado Hayes Standard AT Command Set, es utilizado completa o parcialmente por las fábricas de módems. AT es el código nemotécnico de ATtention (atención), prefijo que inicializa cada orden del módem.

Existen otras normas que los módem deben seguir para que sean estándar, una de ellas es la SERIE V.xx de Hayes, como su nombre lo indica esta regido por los Hayes; la V.42 la cual hace referencia a corrección de errores, mientras que la V.42 bis indica que se tiene corrección de errores y conpresión de datos, hay otras que hacen referencia al tipo de transmisión HALF DUPLEX y FULL DUPLEX etc.

Lista de normas por la CCITT para la serie V.xx

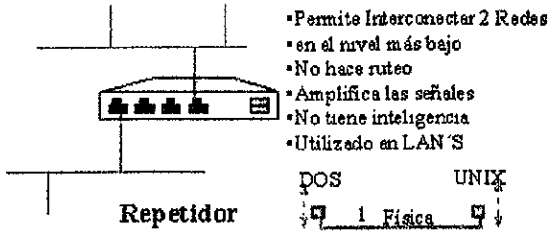
V 110	Estándar CCITT (1984) que especifica cómo el equipo de terminales de datos (DTE) con interfaces seriales asincrónicas y sincrónicas puede ser soportado en una red ISDN Utiliza adaptación de tasa, lo que implica un alineamiento bit por bit entre el DTE y el canal B de ISDN.
V 120	Estándar CCITT (1988) que especifica cómo los DTE con interfaces seriales asincrónicas o sincrónicas pueden ser soportados en una red ISDN usando un protocolo (similar a LAP-D) para encapsular los datos a ser transmitidos. Incluye la capacidad de usar multiplexión estadística para compartir una conexión del canal B entre múltiples DTEs.
V 17	Estándar CCITT (1991) para transmisión por fax que utiliza modulación TCM a 12 000 y 14 000 bps para Grupo 3 Añade TCM al estándar V.29 a 7 000 y 9 600 bps que permiten transmisión en líneas más ruidosas También define funciones especiales (protección de eco, secuencias de apagado, etc) para la operación semiduplex La modulación utiliza una versión semiduplex de V.32 bis
V 21	Estándar CCITT (1964) para módems full-duplex de 0 300 bps, asincrónicos, para uso en líneas conmutadas Utiliza modulación FSK
V 22	Estándar CCITT (1980) para módems full-duplex de 2400 y 1200 bps asincrónicos y sincrónicos, para uso en líneas conmutadas. Utiliza modulación DPSK.
V 22bis	Estándar CCITT (1984) para módems full-duplex de 2400 bps, asincrónicos y sincrónicos, para uso en líneas conmutadas y líneas alquiladas de dos cables con retroceso a operación V.22 de 1200 bps. Utiliza modulación QAM.
V.23	Estándar CCITT (1964) para módems half-duplex de 0- 600 y 0-1200 bps, asincrónicos y sincrónicos, para uso en líneas conmutadas. Tiene un método de transmisión opcional de velocidad dividida, con un canal opuesto de 0-75 bps (1200/75, 75/1200 bps). Utiliza modulación FSX.
V 24	Estándar CCITT (1964) que define las funciones de todos los circuitos para la interfaz RS-232. No describe los conectores o las asignaciones de clavijas esto está definido en ISO 2110 En EE.UU, EIA-232 incorpora la definición de la señal de control de V.24, las características eléctricas de V.28 y los conectores y asignaciones de clavijas definidos en ISO 2110.
V.25	Estándar CCITT (1968) para equipos de llamada y/o respuesta automática en las líneas conmutadas. Utiliza circuitos paralelos y es similar en funcionamiento a los marcadores automáticos RS-366 y Bell 801 usados en EE.UU. El tono de respuesta definido en V 25 es lo primero que se oye cuando se llama a un módem Sirve para la doble función de identificar el equipo de respuesta como un módem, y también inhabilitar el equipo de supresión y cancelación del eco en la red para que un módem full-duplex funcione correctamente.
V 32	Estándar CCITT (1984) para módems full-duplex de 4800 y 9600 bps, asincrónicos y sincrónicos, que utilizan modulación QAM sobre líneas conmutadas o en líneas alquiladas de dos cables Puede agregarse optativamente la codificación TCM V.32 utiliza cancelación de eco para lograr transmisión full- duplex V.32bis es un estándar propuesto en 1990 que extiende V.32 a 7200, 12000 y 14400 bps y agrega características adicionales.
V 34	Estándar de la CCITT para transmisión de datos a 28800, con corrección de error y compresión de datos.
V 35	V 35Estándar CCITT (1968) para módems de bandas de grupos que combinan el ancho de banda de varios circuitos telefónicos para alcanzar altas tasas de datos. V.35 ha llegado a ser conocida como una interfaz RS-232 de alta velocidad más que como un tipo de módem. El conector V.35, grande y rectangular, nunca fue especificado en V 35 pero se convirtió de hecho en estándar para una interfaz de alta velocidad.

Los de dispositivos que permiten interconectar varios segmentos al medio de transmisión para formar una Red mucho más grande, A continuación son descritos brevemente:

Repetidores

Este tipo de dispositivo es muy utilizado en tipos de redes ethernet 802.3 con cableado Coaxial bajo el estándar 10 base5 y 10 base 2, esta norma hace referencia a la implementación de redes indicando que es necesario la instalación de un repetidor para poder cubrir una mayor distancia en el medio de transmisión. La función de este dispositivo es la de amplificar y regenerar las señales electromagnéticas incluyendo obviamente el ruido para ser retransmitidas por el mismo. Estos repetidores también son conocidos con el nombre de amplificadores debido a la función desempañen.

Teóricamente se puede afirmar que no hay limite al utilizados o implementar repetidores en una red LAN, excepto que es muy insano administrar este tipo de red ya que se pueden presentar muchos puntos de falla, los cuales son muy difíciles de detectar ya que tiene que se tiene que revisar tramo por tramo en todo el segmento de la red LAN para encontrarlos.



Concentrador (Hub)

Un dispositivo que une varios canales de comunicaciones en uno solo. Un concentrador es similar a un repetidor pero con varios puertos, físicamente pareciera que se tratara de un equipo con configuración tipo estrella pero lógicamente es un BUS lineal. Son generalmente utilizados con cable UTP nivel 5 ya que cuenta con conectores tipo RJ45, son muy útiles para implementar redes locales y seccionar segmentos de red. Los concentradores se pueden clasificar en 3 tipos: ***Concentradores Pasivos, Concentradores Activo, Concentradores Inteligentes.*** En el primer caso únicamente retransmiten la señal enviada por cada una de las computadoras conectadas al mismo, en el segundo caso los concentradores activos retransmiten y amplifican la señales incluyendo el ruido a lo largo de todo el cableado que se encuentra conectado a cada concentrador; para cubrir una mayor distancia. En el tercer caso concentradores inteligentes aparte de realizar las funciones de un concentrador activo permite realizar swhiche de segmento; esto es se pueden conectar dos o mas segmentos en el mismo concentrador esto indica que cada computadora de cada uno de esos segmentos puede verse entre si, pero esto implica trafico en la red, es aquí cuando actúa el concentrador inteligente ya que puede seleccionar el segmento que será utilizado cuando un paquete es dirigido directamente a una computadora en el segmento. En pocas palabras selecciona la ruta o el segmento donde se encuentra la computadora destino, mientras no se envíen

paquetes a una computadora que no este dentro del mismo segmento no se utiliza tal segmento

Puente (Bridge)

La tecnología básica de un puente (Bridge) se ubica en la capa 2 de ENLACE (LINK) del modelo OSI la cual controla el flujo de datos y el manejo de control de errores, también maneja el control de acceso al medio físico. En otras palabras un Puente permite interconectar dos o más redes LAN que se encuentran separadas y generar una Tabla donde guarda información necesaria (dirección origen, brincos, dirección destino), esta Tabla se le denomina tabla de Ruteo, ara filtrar el trafico de una RED.

Los Puente son por lo general utilizados para dividir el sobre flujo de una red en un segmento separado de la RED.

Un ejemplo muy mencionado es el de tener una red en la cual se tiene demasiado trafico de información ya que se tienen equipos con aplicaciones Autocad y otras accesando bases de datos a un Servidor Novell. La red por consecuencia tendrá tiempos de respuesta muy lentos para los usuarios que quieran correr más aplicaciones sobre la red. Para ello es recomendable dividir la red en dos o más segmentos interconectandolas con un Puente (Bridge) para separar en un segmento el trafico de Autocad y por otro el de las bases de datos, esto mejorara el desempeño de la red. Ya que solo cuando se requiere de accesar una dirección que se encuentre en el otro segmento, esta será filtrada por el Puente y si es valida le permitirá el acceso de lo contrario se quedara en el mismo segmento evitando el trafico del otro lado del segmento.

El concepto direccionamiento y ruteo será visto más a detalle en el modelo OSI.

Debido a su capacidad de filtrado por la dirección de la estación los puentes son usados generalmente para dividir una red muy saturada en dos segmentos por separado. Después de realizar dicha división, el puente evita que el tráfico del segmento alcance otros segmentos.

Hasta en tanto el tráfico del segmento no esté muy saturado, esta estrategia reduce efectivamente el tráfico de cada segmento.

Como ya se a mencionado los puentes permiten interconectar de redes a nivel 2 llamado de Enlace de datos del Modelo OSI y se pueden clasificar en ***Puentes Transparentes, de Traducción, de Encapsulación y de Ruteo de origen.***

Puente Transparente

Proporciona conexión de red a redes que emplean el mismo protocolo en las capas físicas y de Enlace de datos, los puentes transparentes, no representan carga alguna para los recursos, ya que estos no forman parte del proceso de selección de la ruta. Desde el punto de vista del dispositivo, parece que están en una sola red extendida y cada uno se identifica a través de una dirección única.

Para que el puente cumpla con el proceso de traslado de un paquete, requiere la localización de los recursos. Aunque esta información podría configurarse en forma manual, la mayoría de los puentes transparentes cuentan con una función de aprendizaje que emplean para adquirir la dirección del recurso.

El puente aprende las direcciones, y lee la de origen de enlace de datos de cada paquete que llega. Conforme los recibe, crea y actualiza una base de datos (llamada tabla de Ruteo o envío), que contiene una lista de cada dirección de origen de enlace de datos, la conexión del puente en la que ubicó la dirección y un valor de tiempo que indica el momento de la observación. El puente retransmite paquetes sobre la base de las anotaciones en una tabla de envío, una vez que leyó el mensaje, compara su dirección de destino con las direcciones que conserva en la tabla. Si el puente no encuentra la dirección retransmite el paquete en todas sus conexiones (excepto aquella en la que se recibió el paquete) en el caso de establecer varias ala vez, la acción se conoce como desbordamiento.

Diferentes conexiones indican que los recursos de origen y destino no residen en la misma red física. En este caso, el puente envía el paquete basado en la conexión que encontró en la tabla de Ruteo. Los valores idénticos de conexión indican que los recursos de origen y destino se localizan en la misma red, por lo que no será necesario retransmisión.

Puente de traducción

Se puede clasificar como un puente transparente especializado, que proporciona servicios de conexión de red a redes que emplean protocolos diferentes en las capa FISICA y de ENLACE de datos. Los servicios que suministra permiten manipular los paquetes que se asocia a cada tipo de red. El proceso que realiza este puente es relativamente sencillo porque los paquetes Ethernet, Token Ring y FDDI son bastante similares, sin embargo cada tipo de red envía paquetes de diferente tamaño.

Debido a que un puente de traducción no puede fragmentar los mensajes, cada recurso de la red debe configurarse para soportar la transmisión de mensajes de un tamaño que pueda soportar.

Puente de Encapsulación

Otro tipo de puente lo es el puente de encapsulado, el cual se asocia generalmente con las topologías de "red de redes". A diferencia de los puentes de traducción que manipulan en

paquete real de información, los puentes de encapsulado colocan los paquetes que se reciben dentro de un sobre especifico de la red de redes (de ahí el termino de encapsulado), y los envían a otros puentes para su entrega final al receptor.

Puente de Ruteo de Origen

El tercer puente se conoce como puente de Ruteo de origen (SRT;Source Routing). El termino lo utilizó por primera vez IBM para describir un método de unión de Frames a lo largo de las redes Token Ring. El ruteo de origen requiere que el punto de partida del paquete (no el Puente), proporcione la información necesaria para entregarla a su destino.

Dentro de una red de ruteo de origen, los puentes no necesitan llevar tablas de envió. Más bien toman la decisión de enviar o dejar un paquete, con base solo en los datos contenidos dentro del sobe de paquetes. Para instrumentar este esquema, cada recurso de ruteo de origen determina el recorrido para llegar a su destino a través de un proceso denominado descubrimiento de ruta.

Multiplexores

Este tipo de dispositivo permite utilizar un solo medio de transmisión pero implementando a los extremos multiplexaje, esto es que se puede aprovechar mejor el ancho de banda enviando dos o más señales de transmisión por un solo medio de trnasmisón.
Se explicara más a detalle en la capa FISICA (Physical layer) del Modelo OSI.

I.4.2. DISPOSITIVOS DE INTERCONEXIÓN DE REDES.

Este tipo de dispositivos permiten interconectar Redes entre si, entre ellos se encuentran los ruteadores, Brouters, switch y CSU/DSU.

Ruteador (Routers)

A diferencia de los puentes que proporcionan servicios de conexión en la capa de nivel 2 (ENLACE) de datos, los ruteadores hacen lo mismo pero a nivel de la capa 3 (RED), donde las redes conectadas pueden utilizar diferentes protocolos en la capa FISICA y de ENLACE de datos.

En el caso de dos recursos que se comunican a través de una red de un conjunto de redes entrelazadas, la capa de RED proporciona la información necesaria para cambiar y rutear la información a su destino final.

Un Ruteador ofrece servicios más complejos de los que puede suministrar un puente, selecciona activamente la trayectoria entre nodos de origen y destino, y basa su selección en factores tales como costo de transmisión, retraso por tránsito, congestionamiento de red o distancia entre origen y destino del mensaje. La distancia se mide, por lo general, en términos de Hop Count (costeo de saltos), el cual indica el número de ruteadores entre un determinado origen y un destino.

A diferencia de la mayoría de los Puentes, cuyos servicios son transparentes, los servicios de un ruteador pueden ser solicitados explícitamente por un recurso, en consecuencia, un ruteador sólo procesa aquellos mensajes que le dirigen otros recursos. Pero ¿como obtiene un ruteador información acerca de redes distintas y de los ruteadores que intervienen en ellas? y ¿como escoge una trayectoria entre muchas para un mismo destino?.

La respuesta a estas dos preguntas es que los ruteadores se comunican entre sí para compartir información acerca de la red y utilizan protocolos específicos para realizar ese intercambio de información. Este tipo de protocolo es llamado ***protocolo de ruteo.***

Los protocolos corren como un software en un ruteador, constituyendo una tabla de alcnace desde el punto de vista de los ruteadores. Estos protocolos manejan un intercambio dinámico de informacion de ruteo entre todos los que existen dentro de una red. Después de cierto tiempo se dice que el ruteo de red "converge", es decir, todas las tablas de ruteo reflejan el mismo escenario.

Uno de los primeros protocolos de ruteo, el protocolo de información de ruteo (routing information protocol, RIP) se desarrollo para el protocolo XNS, que no es el único en seguir utilizando RIP, sino también IPX y TCP/IP. Este último ofrece otros protocolos incluso el de apertura inicial de trayectoria más corta,(Open Short Path First), OSPF.

Protocolos de Vector distancia: Existen dos tipos de protocolos de ruteo. Los más antiguos, de los cuales RIP constituye un ejemplo, se conoce como protocolos de vector distancia, los cuales hacen publicaciones periódicas que propagan las tablas de ruteo a través de la red. Proporcionan un servicio adecuado para redes pequeñas y relativamente estables, pero no funcionan en redes grandes y/o en crecimiento, donde la difusión periódica de largas tablas añadiría un trafico excesivo y ocupación del ancho de banda de la red.

Protocolo de estado de enlace : Las redes grandes y/o en crecimiento generalmete requieren una nueva genetación de protocolos de ruteo, los protocolos de stado de enlace, y pueden ejemplificarse con OSPF.

A diferencia de los protocolos de vector distancia, estos protocolos no publican emisiones periódicas y talvez repetitivas, sino que envían información de ruteo en forma intermitente y sólo para reflejar los cambios en sus conexiones de red (el estado de sus enlaces). Sin embargo, de las diferencias entre estos dos últimos protocolos, surge otra pregunta : al enfrentar múltiples rutas entre el origen y el destino, ¿que ruta se debe tomar?.

Para un protocolo de vector distancia, la respuesta es simple la misma: la mejor trayectoria es la que ofrece el menor número de ruteadores intermedios o *hops* entre origen y destino.Por el contrario los protocolos de estado de enlace pueden usar múltiples trayectorias para equilibrar el tráfico de mensajes entre os mismos lugares y también ofrecen a los usuarios la capacidad de especificar tres mediciones de ruteo: *tardanza* o *velocidad de transmisión*, *tráfico* o *capacidad*, y *Confiabilidad.*

Los ruteadores tienen acceso a la información desde las tres capas inferiores del modelo OSI (FISICA, ENLACE y de RED) La información de la capa 3 generalmente incluye lo que es llamado un direccionamiento físico de la red. Mientras que el direccionamiento físico a menudo no es asignado por el administrador de la red, el direccionamiento Lógico si lo puede ser. Esta es la diferencia básica entre un puente y un ruteador.

Para reconocer las distintas redes, el ruteador almacena tablas de todas las redes a las que se puede conectar, especificando el número de ruteadores que se deben cruzar para alcanzar. Las tablas de los puentes, en cambio, almacenan las direcciones de todas las estaciones de trabajo. Siendo mucho más grandes que las tablas de Ruteo.

Brouters

Los Brouters son dispositivos híbridos que poseen las características más sobresalientes de ambos equipos (Puente y Router) en un solo dispositivo. Brouters tienen la capacidad de asignar una ruta y por eso se utilizan para usos genéricos, compaces de integrar redes. La función del puente es filtrar información que se encuentra viajando sobre la red, a demás de soportar multiprotocolo esto es varios protocolos de alto nivel al mismo tiempo.

Tomando las características del router su función es generar un mapa de direccionamiento de destinos además de seleccionar una la ruta mas optima para enviar los paquetes de un punto de la red a otro.

DCE

(Data Communications Equipment) equipo para comunicación de datos, o (Data Circuit-terminating Equipment) equipo de terminación de circuitos Un dispositivo de comunicaciones que establece, mantiene y termina una sesión en una red. Puede además convertir las señales para la transmisión, y es tipicamente un módem. Contrástese con DTE.

DTE

(Data Terminating Equipment) equipo terminal de datos Un dispositivo de comunicaciones que actúa como fuente o como destino de las señales en una red. Es típicamente una terminal o una computadora. Nótese la diferencia con DCE.

I.5. MODELOS Y PROTOCOLOS DE RED.

En el caso de los modelos, son creados por organizaciones que tienen a su cargo formar estándares en los modelos y generalizar algunos tópicos acerca de los protocolos de red. Un modelo es Diagrama o dibujo que organiza generalmente las ideas o conceptos para proveer procedimientos de gestión para que sean fáciles de entender. En el caso particular del modelo De redes se describen los servicios requeridos para mover Datos de un punto a otro Para ello es necesario entender que se tienen reglas y el conjunto de estas reglas forman lo que se denomina un protocolo.

OSI (Open System Interconexion,interconexión de Sistemas Abiertos) representa la totalidad de definiciones protocolares y textos asociados adicionales que proveen regularización internacional de muchos aspectos de comunicación que tengan que ver con las conexión de equipos de computo.

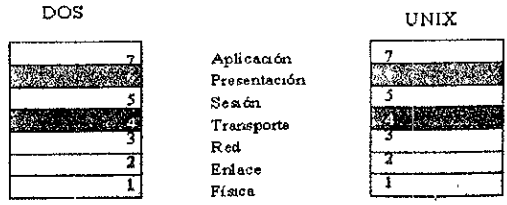
Se comenzaron algunos trabajos por parte de la CCITT en la década de los 70s, pero no era el único organismo que estaba realizando este tipo de investigación sobre el de encontrar un modelo que hiciera referencia a la interconexión de los sistemas abiertos ya que surge en 1997 la ISO. Debido a que ambos organismos CCITT(Comité Consultivo Internacional de Telefonía Y Telegrafía) de y ISO(intenational for Standardization) en sus documentos llegaron a la misma conclusión que podía dividir al modelo OSI en 7 capas. Debido a que ambos documentos tenía similitudes técnicas. La CCITT le propuso a la ISO que el mundo no necesitaba dos documentos iguales para describir un concepto del modelo OSI. Así que esta dos organizaciones se unieron para formar y editar un solo documento que describiera las recomendaciones sobre el modelo OSI para que los equipos de los proveedores pudieran interoperar entre si.

En el presente documento se describen brevemente las 7 capas del modelo OSI así como los conceptos asociados con cada una de las capas.

El presente documento no pretende dar a lujo de detalle como funciona el modelo OSI, pero si de una forma clara entenderlo. Como nota se puede decir que el nombre que CCITT dejo de existir al final de 1992, reorganizandose y ahora se le conoce con el nombre de ITU.

MODELO OSI

Como ya se menciono el modelo OSI esta formado por 7 capas las cuales se explicaran a continuación de manera más detallada.



Modelo OSI

Capa 1 Física (Layer Phisical)

Esta capa es la encargada de implementar reglas para la transmisión de los bits, así como la estructura de la red física que se debe implementar, además de los mecanismos y especificaciones eléctricas que se deben utilizar para ser usados por el medio de transmisión. Algunos de los equipos siguientes son generalmente asociados con la capa física:

Concentradores, hubs y repetidores los cuales generan señales eléctricas. Los conectores para el medio de transmisión, los cuales proveen la interface para interconectar diferentes dispositivos al medio de transmisión.

Los módems son otros dispositivos que permiten un mejor desempeño en la conversión de señalización digital y analógica.

Tópicos ligados a la capa física

A continuacion de describen de manera introductoria los conceptos importantes que se relacionã con la capa física los cuales implican el tipo de conexión, tipo de Topología, tipos de señalización, bit de Sincronía, uso de ancho de banda y multiplexación.

Tipo de Conexión

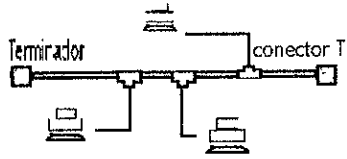
Existen 2 tipos: P*unto a punto, Multipunto*. En el primer caso la conexión es uno a uno ocupando todo el ancho de banda mientras que en el segundo la conexión es uno a muchos y se comparte el ancho de banda. La gráfica muestra como se realiza esto.

Generalmente utilizada en redes SNA.

Tipo de Topología

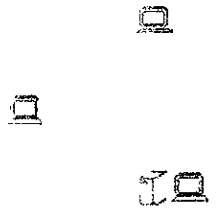
Existen 5 tipos: Bus, Ring, Star, mesh y Cellular entre otras, el tipo de topología indica la forma física en que se encuentran interconectados los equipos.

Bus o Ethernet este tipo de topología es actualmente la más empleada para redes LAN, y se basa en la norma IEEE 802.3. Este tipo de conexión emplea un cable lineal con terminadores en sus extremos y conectores Tipo "T" los cuales conectan a las computadoras, cabe mencionar que la señal eléctrica se distribuye a lo largo del cable. se puede decir que es fácil de implementar, en caso de ruptura no entran las estaciones en red, y requiere menos cable que otras topologías. Se puede utiliar como medio físico Cable coaxial delgado (10base2), coaxial grueso (10base5) y par trenzado (UTP nivel 5, mejor conocido como 10baseT). Incluso Fibra optica 10baseFO utilizando concentradores en las dos ultimas opciones.

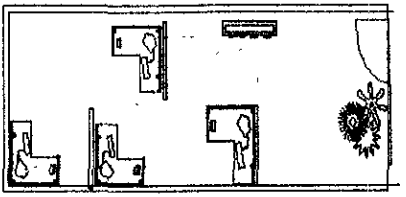


BUS

Ring, topologia similar a un anillo en la cual se interconectan los equipos y utiliza un token que viaja al rededor de anillo va ligada a la norma IEEE 802.6, es fácil de implementar, si se rompe el anillo la red se cae. Puede trabajar a 4 y 16 MB/seg. El equipo utilizado par interconectar los equipos se llama MAU(Multistation Access Unit), unidad de acceso multiple que internamente hace la conexión de anillo.

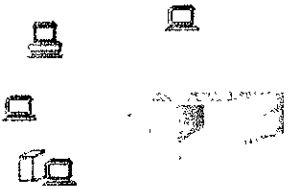


Star. Topología tipo estrella en la cual se conectan varios nodos a una dispositivo central denominado repetidor o concentrador. La conexión física entre cada nodo y el dispositivo central es uno a uno. Es fácil de implemetar, es fácil la detección de fallas, pero es caro por la cantidad de cable que se debe utilizar.



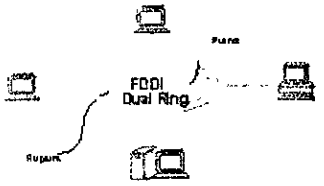
Estrella

Anillo modificado: Actualmente se están utilizando equipos inteligentes que es una modificación de topología de estrella con anillo para evitar la caída de la red, este tipo de topología interconecta a cada uno de los nodos de la red formando una estrella. La señal siempre pasa por el ruteador, típicamente este arreglo utiliza cable par torcido UTP o STP . LA ventaja de utilizar este tipo de topología y no el anillo físico es que si una estación falla o se desconecta el concentrador de inmediato cierra el anillo evitando la caída de la red.



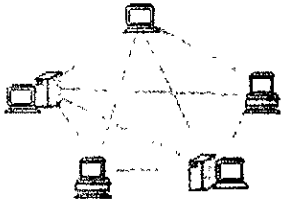
Anillo doble redundante(FDDI): Esta topología fue diseñada para redes que requerían de alta velocidad . La cual consiste en dos anillos de transmisión en contra sentido. El anillo primario es utilizado como canal principal. Si por alguna razón el anillo primario es interrumpido, el secundario restablece la continuidad del primario en forma automática, actuando como redundancia o anillo de respaldo. Se utiliza como medio principal en el cableado de fibra óptica y muy recientemente en cable UTP categoría 5 y cable STP. Con esta topología se pueden alcanzar velocidades de hasta 100MBPS. Algo muy importante es

que aunque se tenga un adoble ruptura esto es en ambos anillos la red no se cae ya que se formarían dos anillos de forma automática.



Anillo Redundante

Mesh: Topología de malla empleada generalmente entre mainframes, cada malla tiene una conexión punto a punto entre todos los dispositivos que componen a la red, es utilizada como medida de seguridad teniendo redundancia en los enlaces, pero entre mas nodos se tengan que conectar se vuelve complicada su administración ya que es fácil perderse entre la maraña de conexiones. Desventajas se pueden mencionar que se requiere una tarjeta por cada cable o enlace, son complicadas para configurarse; ventajas se utiliza para enlaces redundantes, siempre se tiene una ruta alterna.



Cellular, este tipo de topología tiene pocos años de ser empleada y va ligada al concepto de redes inalámbricas de conexión punto apunto o punto a multipunto. Funcional de forma similar a la telefonía celular en donde un usuario se encuentra en movimiento y conectado a una célula, mientras se mueva de célula, esta ultima le informa ala central de que se cambio de célula y le siga envinado datos a su computadora, a este concepto se le conoce como Rooming

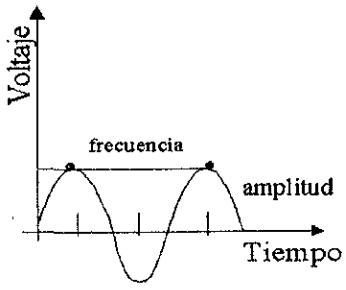
Señalización Digital / Analogica

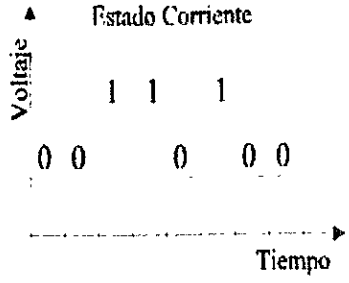
Esto no es otra cosa que la forma en que se representan los datos a nivele electricos o de impulsos que representan un estado o bien la transición de un nivel de 0 o 5volts, representados por unos y ceros

En el caso de las señales digitales se utiliza un esquema de codificación llamado estado corriente el cual se puede subdividir en Unipolar, polar, retorno a cero(RZ). Mientra que el esquema utilizado en señales analógicas es utilizar señales de onda electromagnéticas para

representar los estados ceros y unos variando la amplitud, frecuencia y fase, esto es en el caso de amplitud si la amplitud aumenta representa un (uno), si la amplitud disminuye se representa con un (cero),mientras que en frecuencia aumenta se representa con un (uno), así también para el caso de la fase si esta se adelanta 90° representa un uno, así entonces si se retrasa se representa con ceros.

En conclusión se puede decir que existen varia formas para representar dos Estads (cero /unos) llamado Binario.





Bit de Sincronización

Es un tópico que se requiere en la capa física para cualquier medio de transmisión de datos y se utilizan generalmente dos tipos, Asíncrono y Síncrono, para el primero transmisión Asíncrona una Transmisión de datos en la que cada carácter es una unidad auto-contenida con sus propios bits de comienzo y final, y los intervalos entre caracteres pueden no ser uniformes. Es el método más común de transmisión entre una computadora y un módem, aunque el módem puede ser conmutado a transmisión síncrona para comunicarse con el otro módem. También llamada transmisión arranque/parada (start/stop transmission). Para el segundo caso transmisión sincrónica se tiene una transmisión de datos en la que ambas estaciones están sincronizadas. Se envían códigos desde la estación transmisora hacia la receptora para establecer la sincronización, y se transmiten entonces los datos en corrientes continuas. Los módems que transmiten a 1200 bps o más convierten, frecuentemente, las señales asíncronas provenientes del puerto serie de una computadora en una transmisión síncrona con el otro módem, una ventaja de la transmisión síncrona es que pueden manejarse mayores velocidades en la transmisión.

Ancho de banda y Multiplexaxión,

El ancho de banda y la multiplexación de datos son también dos conceptos que se cubren en la primera capa del modelo OSI y simplemente se van a comentar para el caso del ancho de bando cabe señalar que el uso de un canal dedicado de datos se le llama banda base el cual ocupa todo el ancho de banda, mientras que cuando se comparte parcialmente el canal en subcanales se denomina Broadband y generalmente es utilizado con señalización analógica.

Ahora bien para el caso del multiplexaje se utiliza cuando se tiene un solo canal de enlace y se requiere conectar mas terminales o equipos esto es compartiendo el medio de transmisión y esto se logra con dispositivos llamados multiplexores que realizan la función de separar la señales utilizando algunas técnicas como la de FDM(Frecuency-Division Multiplexing) conocida como Multiplexación por división de Frecuencia, TDM(Time- Division Multiplexing) conocido como Multiplexación por División de Tiempo. Y por último StartTDM(Statical- TimeDivision Multiplexing) Multiplexación por división de tiempo estático.

Capa 2 de Enlace de Datos (Data Link Layer)

Esta segunda capa de enlace de datos llamada Data link Layer se ocupa de la forma en como serán transmitidos los datos ahora llamados (Frames o Paquetes) a la capa Física o de acceso al medio. También esta encargada de detectar corrección de errores, Control de Flujo de datos así como de identificar las computadoras que se encuentran en la RED. En esta capa operan los Bridges, Hubs Inteligentes, Tarjetas de RED, y adaptadores..

La IEEE a subdividido esta capa de enlace de datos en 2 subcapas denominadas Data Link MAC(Medio Acces Control) o bien llamada Control De acceso al Medio y la de Data Link-LLC(Control de enlace de datos) son los responsables de asegurar que los bits recibidos son los mismos que los bits enviados. En estas 2 subcapas se encuentran ligados algunos tópicos importantes que serán descritos a continuación Brevemente.

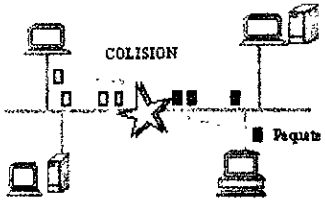
Tópicos ligados a la CAPA FISICA

Subcapa MAC y LLC

Esta subcapa capa se encarga de implementar reglas de control para la transmisión de datos sobre el medio de transmisión, el proceso de control es llamado acceso al medio. Cuando no se tiene un control en una red, los paquetes de petición se encuentran viajando al lo largo de la red provocando choches de señales, a estos se les denomina colisiones, los cuales deterioran o atenúan la señal. En una red no se puede tener control a menos que se implementen reglas para evitar estas colisiones. Para esto existen algunos métodos que lo permiten y son:

Contensión Este basado en la retransmisión de señales esto es cuando las estaciones transmiten al mismo tiempo se genera una colisión. Para reducir el número de colisiones se utilizan dos tipos de protocolo llamado CSMA (Carrier sence multiple acces protocol), pero no los elimina. Cuando se aumenta el número de estaciones en la red, también se incrementa geométricamente el número de colisiones. Este sistema de contención se recomienda generalmente en redes que tengan poco tráfico de datos. Ejemeplos de protocolos de contención se encuentran el CSMA/CD (Collision Detection) y el CSMA/CA(Collision Avoidance).*Un método de acceso en banda base que emplea una técnica de detección*

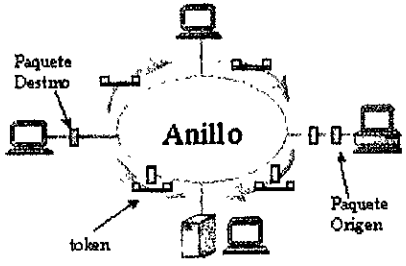
decolisiones. Cuando un dispositivo trata de ganar acceso a la red, verifica si la misma está libre.Si no lo está, espera una cantidad aleatoria de tiempo antes de intentarlo nuevamente. si la red está libre y dos dispositivos tratan de ganar acceso exactamente al mismo tiempo, ambos se retractan para evitar una colisión y luego cada uno de ellos espera una cantidad aleatoria de tiempo antes de reintentarlo.



Contensión

Paso de Señal (Token-Pasing)

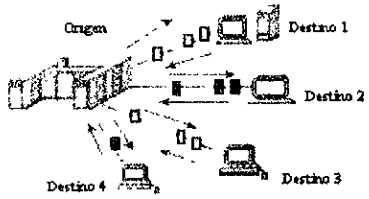
Este Método de acceso emplea repetición continua de envío de una señal llamada (token) que es transmitida a través de la red. Cuando una terminal o computadora desea enviar un mensaje, espera un señal vacía. Cuando encuentra una, la completa con la dirección de la estación de destino y una parte con la totalidad del mensaje. Todas las computadoras y terminales de la red verifican constantemente las señales que pasan para determinar si hay algún mensaje para ellas, en cuyo caso "toman" el mensaje y pasan la señal al estado de vacía. El paso de señales utiliza topologías bus y de anillo. Una analogía de la cual se puede hacer referencia es la rueda de la fortuna, la cual se encuentra girando y hasta que una persona desea subir se solicita el acceso, cuando se detiene la rueda se vacía la canastilla, y se sube la nueva persona y así repetidamente. Este método elimina totalmente las colisiones, pero es un poco más complicado de configurar cada vez se añade una nueva terminal. Por otra parte va muy ligada a la topología de Anillo.



Token Passing

Poleo (Polling)

Es otro método de acceso al medio que esta formado por 2 tipos de dispositivos llamados (Controlador primario o maestro) y los de tipo Secundario los cuales dependen del primario. Cuando un secundario requiere servicio, le envía una petición al primario que siempre se encuentra poleando si alguien necesita el servicio, es entonces cuando se establece una transmisión entre el secundario y el primario, una vez que se termina la transmisión el primario polea la siguiente estación secundaria. Este tipo de acceso es utilizado generalmente en redes que tienen mucho trafico.



Poleo

Direccionamiento,

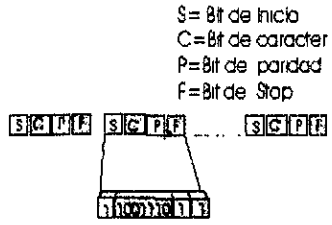
La capa de enlace la cual se encargada también del direccionamiento de datos a nivel Físico, este es otro concepto que es muy importante. Actualmente los fabricantes de hardware colocan una dirección única en cada dispositivo que sale al mercado. Este número es único y garantiza que no existirá uno igual en el mundo. Este número es llamado MAC ADDRESS y esta formado por la identificación del fabricante y el número asignando al dispositivo. Entonces LA capa 2 se encarga de identificar por la red el origen y el destino utilizando esta MAC Address asignada a cada dispositivo.

Subcapa LLC

Como se describió anteriormente la capa 2 o de enlace permite tener dos subcapas la de MAC que se encarga del acceso al medio de transmisión así como el direccionamiento, mientras que en la subcapa de LLC se encarga mantener y establecer el enlace de un dispositivo a otro en otras palabras se encarga de la sincronización de la transmisión y de los servicios de conexión. Los métodos que se utilizan par a ellos son transmisión (sincrona, asincrona) y la de (Control de flujo, Control de errores) para la conexión de servicios. El estándar de la IEEE_802.2 hace referencia al Control de enlaces lógicos que define el protocolo que asegura que los datos se transmiten de forma fiable a través del enlace de comunicaciones LLC(Logical Link Control).

Bien para el caso de la transmisión asincrona se requiere de un bit de inicio, el carácter, un bit de paridad y un bit de parada, en este caso los dispositivos que se conectan tiene su propio reloj pero no se sincronizan, una ventaja de utilizar este tipo de transmisión es que es más barato pero el dato que se transmite crece considerablemente ya que sele agrega heders (cabeceras de señalización). Mientras que para el caso Sincrono los relojes se sincronizan y pueden enviar mas datos a velocidades mayores, también utiliza un bit de CRC(Cyclical

Redundance Check) para tener un mejor desempeño en la detección de errores. Para el caso de manejo de control de flujo se utilizan dos métodos que son el de Ventana Fija y el de Ventana Estática.



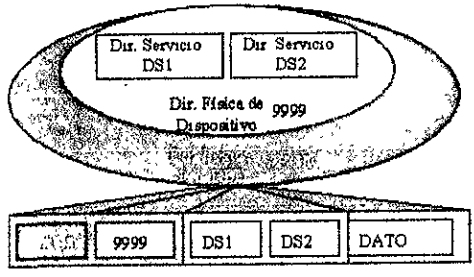
Transmisión Asincrona

Capa de Red (Network Layer)

La capa tres (RED) del modelo OSI se encarga del direccionamiento lógico, del swicheo, del descubrimiento de rutas, selección de rutas, de los servicios de conexión y de los servicios de Gateway.. Cada uno de estos tópicos son descritos a continuación así como los métodos utilizados en cada uno.

Tópicos relacionados con la capa de red Direccionamiento

Existen dos tipos de direccionamiento en la capa de red el Lógico y el de servicio; el direccionamiento lógico de red indica el tipo de red origen o destino, mientras que el direccionamiento de servicio especifica un proceso o una aplicación que se encuentra corriendo en una computadora origen o una computadora destino. Existe otro tipo de direccionamiento el cual indica la dirección física del dispositivo(computadora). El direccionamiento de servicio es también llamado (Puerto o Socket) el cual es especificado por algún protocolo.



Direccionamiento de Servicio

Conmutación (Swiching)

La capa de red también se encarga de proveer una ruta o canal entre dos estaciones que desean intercambiar información para esto se utilizan 3 técnicas la de (Conmutado de Circuitos, Conmutación de mensajes y la de conmutación de paquetes),La primera indica que se utilizan un canal dedicado mientras se establece la comunicación y después se envía el o los paquetes, cancelando el enlace una vez terminada la conversación, una analogía o similitud es la conmutación telefónica la cual establece una conexión entre dos usuarios y esta existe mientras se tiene la conversación. La segunda técnica de conmutación de mensajes no establece una ruta dedicada entre dos estaciones de trabajo para establecer una conversación. Las conversaciones son divididas en mensajes que tienen su propia dirección destino; en otras palabras la computadora origen genera y almacena los mensajes y después se transmiten a cada computadora destino. La tercera técnica Conmutación de paquetes utiliza las ventajas de ambas técnicas la de conmutación de circuitos y la de conmutación de mensajes. Pero además esta técnica de conmutación de paquetes se subdivide en dos que es la de utilizar Conmutación de Datagramas y la de Conmutación Circuitos Virtuales, en estos dos últimos casos son necesarios dos direcciones la de Origen y Destino., además de subdividir los mensajes en paquetes y cada paquete contiene la dirección origen, destino así como parte del mensaje. En el caso de la conmutación de circuitos virtuales se establece una conexión Lógica entre la dirección origen y la de destino mientras se establece la conversación.

Descubrimiento de Rutas (Route Discovery)

El Descubrimiento de Rutas es un proceso para identificar rutas y mantener o actualizar tablas de ruteo, estas tablas de ruteo son listas que contiene información de el número de saltos que se deben realizar para llegar a otro segmento de red; así como una lista de direcciones de los dispositivos origen y destino que se encuentran en la red, así como un costo o penalización por usar determinada ruta. Esta penalización puede ser en base al número de saltos, a la cantidad de tiempo y la penalización en cuanto a costo por utilizar una determinada ruta antes de llegar a su destino. Existen dos métodos para descubrir rutas, uno de ellos es el llamado Vector Distancia (distance vector) y el Estado Enlace (Link-State), En el primer caso protocolo de vector distancia, envía una tabla de ruteo de la red a otros ruteadores que se encuentran en el mismo segmento de red, cada ruteador construye su propia tabla de ruteo. Mientras que en el caso del protocolo Estado de enlace los ruteadores loa cuales descubren una ruta identifican la red a la cual se encuentran conectados (Athach), recibiendo una tabla de ruteo inicial del ruteador Local. La diferencia entre estos dos tipos de protocolos es que en este ultimo el router notifica o envía los cambios que han ocurrido en las tablas a los otros ruteadores.

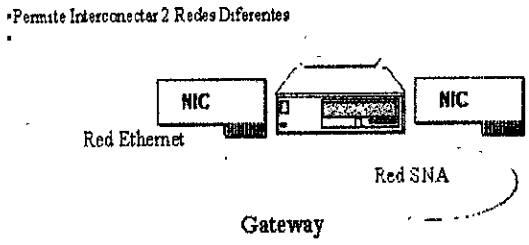
Selección de Ruta (Route Selection)

La selección de ruta es otro concepto importante dentro de la capa de Red. Una vez que se han construido las tablas de direccionamiento (ruteo) en los ruteadores. Es necesario seleccionar una ruta, esta ruta puede ser Dinámica o Estática . En el primer caso son los ruteadores los que establecen la mejor ruta en base a un costo o penalización o bien por el número de saltos al cruzar determinadas rutas; estas rutas pueden cambiar como su nombre lo indica dinámicamente. Mientras que en el caso de selección de una ruta estática se basa en la definición por parte del administrador en cada dispositivo una ruta fija, en otras palabras un ser humano es quien crea en los ruteadores las tablas de Direccionamiento (ruteo) para que los nodos utilicen únicamente determinada ruta.

Servicios de Conexión (Connection Services)

Getway services

El servicio de GateWay en la capa de red es responsable de fragmentar y posteriormente ensamblar los paquetes de datos que van de una red a otra en un tamaño aceptable para ambas redes. Entendiéndose que estas redes son diferentes. El Gateway ajusta el tamaño de los paquetes de datos, otra de sus funciones es la de implementar e interpretar las reglas de dos redes diferentes, el caso de una red SNA con una Novell o TCP/IP. En otras palabras Un Gateway permite interconectar dos tipos de redes disimiles.



Capa de Trasporte (Trasport Layer)

TRANSPORTE - Es el responsable de la validez e integridad de la transmisión, de un extremo a otro. Los servicios de transporte OSI incluyen los estratos 1 a 4, los que son colectivamente responsables del tránsito de los bits de la estación emisora a la estación receptora.

Capa de Sesión (Session Layer)

Se encarga de proporciona la coordinación de las comunicaciones en una forma ordenada. Por ejemplo, marca partes significativas de los datos transmitidos para asegurarse que el mensaje completo fue recibido correctamente. Para realizar esto se utilizan algunos métodos que se describen a continuación en tópicos ligados esta capa como son el de Control de Dialogo y la Administración de la Sesión.

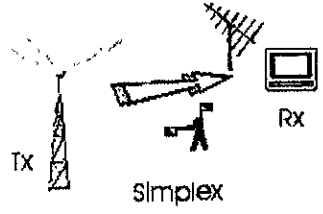
Tópicos ligados a la Capa de Sesión

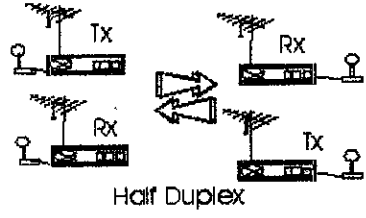
Control de Dialogo

Existen 3 tipos distintos de control de dialogo los cuales describen la dirección y el sentido por el cual los datos fluyen, estos métodos de control de flujo son el Simplex, Half-Duplex y el Full-Duplex.

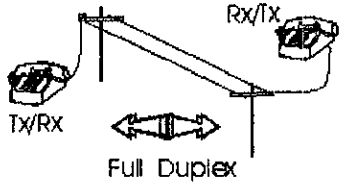
***Simplex-Dialog*:** Es un método que permite únicamente la comunicación del dialogo en un sentido, esto es permitiendo tener solo un emisor y uno o varios receptores, pero los receptores no pueden de ninguna manera poder ser emisores. Ejemplo de esto es la TV. La Radio.

Half Duplex Dialog: Es otro método que permite la comunicación en ambos sentidos desde el punto de vista de dialogo, esto es que ambos pueden ser emisor y receptor pero sin transmitir al mismo tiempo, para ello es necesario que el que actúa como receptor debe esperar a que termine el dialogo del emisor para poder convertirse entonces en transmisor y el que actuaba como emisor pasar a ser receptor. Así alternadamente. Una analogía a este tipo de dialogo es la empleada en las transmisiones de radio ciudadanas CB.





Full-Duplex-Dialog: es el tercer método empleado en el control de Dialogo el cual implica una transmisión en ambos sentidos al mismo tiempo; para que se lleve a cabo este tipo de transmisión es necesario contar con 2 canales para que por uno se utilice para transmitir y el otro para recibir.



Administración de la Sesión

La administración de sesión es un servicio que realiza la capa de sesión, esta administración esta seccionada en las siguientes tareas: el establecimiento de la conexión, la transferencia de datos y la finalización de la conexión. La administración de la conexión de sesión se encarga de verificar entre otras las siguientes subtareas: verificación de Nombre de Usuario y Password, los números de conexiones establecidas, también se encarga de administrar los servicios que son requeridos y su tiempo de duración, además de saber cual estación que inicio la conversación así como coordinar el procedimiento de retransmisión para informarlo a la capa inferior (Transporte).

La subtarea de transferencia de datos: se encarga de mantener la conexión o la comunicación así como pasar los mensajes entre dos entidades (computadoras, nodos, dispositivos).

La subtarea de Desconexión: se encarga de finalizar la comunicación de la sesión, una analogía de esto es cuando se termina una conversación telefónica cuando se dice "Bye" o se levanta la bocina, esto significa utilizar una bandera para informar que la comunicación de la sesión finalizo.

Capa de Presentación (Presentation Layer)

Esta capa se encarga de Negocia y administra la forma en que se representan y codifican los datos. Provee un común denominador para la transferencia de datos de diferentes sistemas, ASCII, EBCDIC, binario, etc. Tiene dos funciones especificas una la de traducción y la de encriptación de mensajes entre la capa de sesión y la capa de aplicación.

Algunos de los métodos utilizados para la traducción son el de traducción por Ordenamiento de Bit, traducción por ordenamiento de Byte y el de traducción de código de carácter

La traducción por ordenamiento de bit es empleado para identificar y poder informar a la capa superior e inferior cual es el sentido que se debe utilizar para poder interpretar un dato. Ejemplo de esto es cuando una computadora manda un caracter este pudo ser enviado con un tamaño de 2, 4, 7,8,16 o 32 bit de longitud , pero no será el mismo dato si se le el carácter de izquierda a derecha que de derecha a izquierda. Y este método se encarga de realizar esta función de identificación del sentido para representar un carácter.

La traducción por ordenamiento de byte utiliza el concepto de bit más significativo y el de menos significativo para indicar por donde se debe iniciar la traducción.

La traducción por código de carácter es el encargado de traducir de un estándar ASCII a un estándar EBCDIC y viceversa.

Capa de Aplicación (Application Layer)

La capa 7 de aplicación se encarga de proveer el protocolo necesario para tener un mejor desempeño de los servicios de red mientras que las capas inferiores (capa de presentación a la capa física) se encargan de las tareas así como de las tecnologías que soportan los servicios de la capa de Aplicación (capa 7). Esta capa entonces se encarga ***de los servicios de red*** vistos al inicio de este capitulo como son: Servicios de Archivos, Servicios de Impresión, Servicios de Bases de Datos, Servicios de mensajes entre otros.

Esta capa También se encarga un servicio de ***anunciamiento*** el cual puede ser del tipo ***activo o pasivo;*** los cuales son dos métodos diferentes de anunciamiento, en caso del Activo un servidor. El cual provee el servicio envía periódicamente un mensaje, el cual incluye la dirección del servicio a la RED. Para el caso del pasivo, este servicio se encuentra en el servidor como un directorio compartido, cuando una PC requiere del servicio simplemente van al directorio y obtiene la dirección del servicio.

Existen también otro termino importante en esta capa de aplicación el cual indica el método de uso del servicio, este termino indica como es que se alcanza a la aplicación o servicio, y esto es tarea del sistema operativo ya sea local, remoto o colaborativo. En el caso local cuando el sistema operativo detecta que se trata de una aplicación que se encuentra en la computadora local lo invoca., pero sino se encuentra este envía un mensaje a la red, dejándole al sistema operativo de red dicha tarea de la búsqueda.

Ejemplo : cuando se dan los siguiente comandos DIR , NDIR , ls -l

Cabe señalar que las capas del modelo OSI interactúan entre si con las capas inferiores, esto es cada vez que se (sube / baja) un nivel se (agregan / quitan) cabeceras al Frame (paquete), también se puede señalar que los nombres de paquetes pueden tener cualquier nombre. Realizando una analogía se puede comparar con una conversación, ejemplo de esto se describe en la tabla siguiente.

Capa	Se encarga de crear	Analogía
7 de aplicación	Messages/Packets	Conversación
6 de presentación	Packets	Dialogo
5 de sesión	Packets	Párrafos
4 de transporte	Dtagrams/Segments/Packets	Oraciones
3 de RED	Datagrams/Packets	Frases
2 de enlace de datos	Frames/Packets	Palabras
1 Física	Bits/Packets	Letras

Uno se preguntara como usuario para que nos sirve esto del modelo OSI , ya que es un tanto intangible, además de ser un poco complicado de entender, bueno pues se cree que si se comprenden estos términos se podrán comprender muchas de las revistas que implican términos de computación, así como saber bajo que términos se debe construir algún dispositivo o interfaces si se quiere conectar a un equipo o computadoras. O bien para crea programas que requieran convivir con otros ambientes o sistemas operativos y que estos funcionen entre otros.

I.6. ESTÁNDARES.

NORMAS IEEE 802 PARA LAN

Los comités 802 del IEEE se concentran principalmente en la interfaz física relacionada con los niveles físicos y de enlacede datos del modelo de referencia OSI de la ISO. los productos que siguen las normas 802 incluyen tarjetas de la interfaz de red, bridges, routers y otros componentes utilizados para crear LANs de par trenzado y cable coaxial. el nivel de enlace se divide en 2 subniveles MAC y LLC. son diferentes en la capa física en la subcapa MAC, pero son compatibles en la subcapa de enlace. es un módulo de software incorporado a la estación de trabajo o al servidor que proporciona una interfaz entre una tarjeta de interfaz de red NIC y el software redirector que se ejecuta la computadora..

802.1- Da una introducción al conjunto de normas y define las reglas de interfaz, para interconexión de redes. Esta define la relación entre las normas 802 del IEEE y el modelo de referencia de la OSI. este comité define que las direcciones de las estaciones de la LAN sean de 48 bits para todas las normas 802, así cada adaptador puede tener una única dirección.

802.2. Describe la parte superior de la capa de enlace que utiliza el protocolo LLC. La cual define el protocolo de Control de enlaces lógicos que asegura que los datos se transmiten de forma fiable a través del enlace de comunicaciones LLC Logical Link Control. en los bridges estos dos subniveles se utilizan como un mecanismo modular de conmutación. a un frame que llega a una red Ethernet y se destina a una red Token Ring , se le desmonta su header de frame ethernet y se empaqueta con un header de Token Ring. el LLC suministra los siguientes servicios: servicio orientado a la conexión en el cual se establece una sesión con un destino y se libera cuando se completa la transferencia de datos. servicios orientados a la conexión con reconocimiento parecido al anterior, en el cual se confirma la recepción de los paquetes. servicio sin reconocimiento no orientado a la conexión en el cual no se establece una conexión ni se confirma su recepción.

802.3 describe la norma CSMA/CD. se utilizan en redes LAN con protocolo CSMA/CD. Históricamente se inicia en el sistema ALOHA en Hawai, continuándose su desarrollo por la XEROX y posteriormente entre XEROX, DEC e Intel proponen una norma para la ethernet de 10 Mbps la cual fue la base de la norma 802.3 hay dos tipos de cable: ethernet grueso con marcas para los conectores cada 2,5 metros y el ethernet delgado, coaxial flexible de 50 ohm, con conectores BNC y en otros casos, cable trenzado 10baseT conconectores RJ-45. la

longitud máxima permitida para el cable de la 802.3 es de 500 metros (coaxial grueso). para aumentar su extensión se utilizan repetidores.

802.4 describe la norma token bus, debido a problemas inherentes del CSMA/CD como la característica probabilística de su protocolo que podría hacer esperar mucho tiempo a un frame, o la falta de definición de prioridades que podrían requerirse para transmisiones en tiempo real, se ha especificado esta norma diferente. La idea es representar en forma lógica un anillo para transmisión por turno, aunque implementado en un bus. Esto porque cualquier ruptura del anillo hace que la red completa quede desactivada. Por otra parte el anillo es inadecuado para una estructura lineal de casi todas las instalaciones.

El token o testigo circula por el anillo lógico. Sólo la estación que posee el testigo puede enviar información en el frame correspondiente. Cada estación conoce la dirección de su vecino lógico para mantener el anillo. Protocolo de subcapa MAC para 802.4 token bus al iniciar el anillo, las estaciones se le introducen en forma ordenada, de acuerdo con la dirección de la estación, desde la más alta a la más baja. El testigo se pasa también desde la más alta a la más baja. Para transmitir, la estación debe adquirir el testigo, el cual es usado durante un cierto tiempo, para después pasar el testigo en el orden adquirido. Su una estación no tiene información para transmitir, entregará el testigo inmediatamente después de recibirlo. La estructura del frame para un 802.4 es: el preambulo es utilizado para sincronizar el reloj del receptor. los campos correspondientes a los delimitadores de comienzo y fin del frame contienen una codificación analógica de simbolos diferentes al 0 y 1, por lo que no pueden aparecer accidentalmente en el campo de datos.

802.5 describe la norma token ring..Una de sus características es que el anillo no representa un medio de difusión sino que una colección de enlaces punto a punto individuales. Seleccionada por la IBM como su anillo LAN.

802.6 red de área metropolitana MAN.Define un protocolo de alta velocidad en el cual las estaciones enlazadas comparten un bus doble de fibra óptica que utiliza un método de acceso llamado bus dual de cola distribuida o DQDB Distributed Queue Dual Bus. DQDB es una red de transmisión de celdas que conmuta celdas con una longitud fija de 53 bytes, por lo tanto, es compatible con la ISDN de banda ancha ISDN-B y ATM. la conmutación de celdas tiene lugar en el nivel de control de enlaces lógicos 802.2.

802.7 grupo asesor para técnicas de banda ancha. Proporciona asesoría técnica a otros subcomités en técnicas de conexión de red de banda ancha.

802.8 grupo asesor para técnicas de fibra óptica. Proporciona asesoría técnica a otros subcomités en redes de fibra óptica como alternativa a las redes actuales basadas en cobre.

802.9 redes integradas para voz, datos y vídeo. Tanto para LANs 802 como para ISDNs. la especificación se denomina IVD Integrated Voice and Data. el servicio proporciona un flujo multiplexado que puede llevar información de datos y voz por los canales que conectan las dos estaciones sobre cables de par trenzado de cobre.

802.10 seguridad de red. grupo que trabaja en la definición de un modelo normalizado de seguridad que interopere sobre distintas redes e incorpore métodos de autentificación y de cifrado.

802.11 redes inalámbricas. comité que trabaja en la normalización de medios como la radio de amplio espectro, radio de banda angosta, infrarrojos y transmisiones sobre líneas de potencia.

802.12 LAN de acceso de prioridad bajo demanda (100VG-AnyLAN). Comité que define la norma ethernet a 100 Mbps con el método de acceso de prioridad bajo demanda propuesto por la Hewlett Packard y otros fabricantes. el cable especificado es un par trenzado de 4 hilos de cobre utilizándose un concentrador central para controlar el acceso al cable. Las prioridades están disponibles para soportar la distribución en tiempo real de aplicaciones multimediales. Los concentradores 100VG-AnyLAN controlan el acceso a la red con lo cual eliminan la necesidad de que las estaciones de trabajo detecten una señal portadora, como sucede en el CSMA/CD de la norma ethernet. cuando una estación necesita transmitir, envía una petición al concentrador.

Todas las transmisiones se dirigen a través del concentrador, que ofrece una conmutación rápida hacia el nodo destino. Emisor y receptor son los únicos involucrados en las transmisiones, a diferencia del CSMA/CD donde la transmisión es difundidad por toda la red. Si múltiples peticiones de transmisión llegan al concentrador, primero se sirve la de mayor prioridad. Si dos estaciones de trabajo hacen la solicitud con la misma prioridad y al mismo tiempo, se van alternando para darles servicio. Este método de trabajo es mejor que CSMA/CD.

CAPITULO II JUSTIFICACION POR LA QUE SE DEBE IMPLEMENTAR UN CENTRO DE CONTROL.

II.1. NECESIDAD DE INTEGRAR Y MONITOREAR UNA RED.

Para implementar algún sistema de seguridad en primera instancia es necesario definir que se quiere proteger , visto de otra forma que es tan importante para nosotros o para la empresa que representamos o bien para la cual trabajamos lo que queremos proteger. En este caso, Información la cual es esencial para nosotros y para los usuarios que utilizan la red como medio de transporte para intercambiar información y conectarse a bancos de datos entre otros.

Una vez que se a planteado que es lo que se quiere proteger en el caso de una Red Publica en particular X compañía es necesario tener seguridad sobre la red de datos. En particular la red la podemos subdividir o catalogar de acuerdo su nivel de importancia: Mainframe, Red, Intranet, Internet

En el caso de un Mainframe existen grandes cantidades de información las que hay que proteger , además de las aplicaciones que se encuentran corriendo en línea con una gran cantidad de usuarios conectados al mismo que ofrecen a su vez un servicio. El detener estas aplicaciones a horas pico del día provocaría una caos terrible y un descontento en las personas que reciben dicho servicio.

La intranet y la internet al igual que en el caso del mainframe se sirven de la infraestructura de una red publica y es por ello también que se deben tomar medidas de seguridad para y monitorear los eventos o alarmas que se susciten antes de que se presenten los problemas, esto con la finalidad de tener un mejor desempeño de red, así como de los servicios que se ofrecen.

Compañías dedicadas a cuestiones de seguridad indican que casi el 70% de las ocasiones entre otras. Por las que una compañía sufra algún tipo de sabotaje o perdida de información es debida generalmente por personal que a sido despedido y que realizan acciones en contra, como llevarse o más aun borrar informe.

El otro 20% de las causas son diversas o variadas y van desde , caídas de energía las cuales pueden provocar mal funciona miento del equipo, no cambiar los password periódicamente, no tener la precaución de quitar o cambiar privilegios al usuario GUEST o ANONYMOUS en los ruteadores etc.

Otras razón es la que algunos usuarios no visualizan la importancia que implica el termino seguridad, prestado sus USERNAME y PASSWORD a otros usuarios para entrar a los sistemas.

Caso concreto de la implementación de un centro de control para x compañía se consideran 3 puntos importantes para proteger y es el tipo de red, para este caso la RED NOVELL, LA

RED TCP/IP (UNIX servidores entre los cuales se encuentran equipos MINIS) como son AS400 y Maninframes. Y en cada una de estas redes es importante la información y los procesos que en los equipos se encuentran corriendo.

Un punto muy importante que considerar es el echo de que los tres ambientes puedan convivir en una red Coorporativa, la cual es parte de implementación de nueva tecnología para realizarlo. Esto será explicado en el capitulo tres y cuatro como es posible esto.

II.2. ACCESO AL MAIN FRAME.

Cuando se Habla de MainFrames es un tanto difícil de interpretar algunos conceptos, pero no se debe de perder de vista que se trata de otra computadora que comparte sus recursos y que realiza procesos.

En el capitulo siguiente se describe más a detalle los elementos que conforman una red SNA y algunos conceptos que la conforman.

Mientras tanto se puede comentar que en un ambiente SNA (System Network Arquitecture) existen los HOST o maquinas anfitrionas en donde se realizan las operaciones o transacciones y que fue desarrollada y presentada por IBM en 19874. La redes SNA están compuestas por una variedad de productos de hardware y software que interactúan todos entre sí. La red SNA esta formada a demás por controladores denominados tipo 4, y terminales e impresoras denominadas de Tipo 2.

No se debe de perder de vista el tipo de acceso al MainFrame, Esto es una conexión LU tipo 2. Esto es una conexión nodo con un anfitrión o HOST, esto se realizaba a través de un medio de transmisión vía enlaces privados con terminales Remotas y cable coaxial para terminales locales.

Por lo que su momento fueron funcionales pero llega un momento en que el acceso y la administración de la red se vuelven lentos y esto es debido a la carga de servicios y de terminales que se van adicionando a la RED.

Es por ello que se debe pensar en otras alternativas para un mejor funcionamiento y administración de la RED.

II.3. SERVICIOS QUE OFRECE.

Dentro de un ambiente de RED SNA , El Mainframe es parte importante pero no lo es tanto sino se tienen servicios o aplicaciones que procesen información , en este caso altas cantidades de información requieren de igual forma un procesamiento y una carga de trabajo pesado, pues ya que para eso fueron diseñados.

Algunos de estos servicios son :

Sistemas manejadores de Bases de datos como el llamado DB2. El cual es un sistema para el manejo de grandes volúmenes de información. Y un gran número de usuarios lo utiliza diariamente, para consultar información en línea.

Sistemas de Procesamientos por lotes. El cual consiste en un archivo el cual contiene una serie de instrucciones o comandos que se procesan o ejecutan de manera secuencial, esto es de comando en conmando se le va pasando al MainFrame para que sea procesado durante una fecha u hora predeterminada, por el operador.

Transacciones con centrales telefónicas vía FTP, Existen otro tipo de procesos que se encuentran corriendo a diferentes tiempos esto es según la carga de trabajo de las centrales telefónicas, pero por lo regular lo realizan durante la madrugada, el cual consiste en enviar la tarifación o la cobranza etc. vía un FTP (FILE TRANSFER PROTOCOL) esto es el envió de archivos a través de paquetes al HOST para que sean procesados y clasificados.

Servicios de Impresión. Es otra de las principales características de un MainFrame que soporta muchisimas conexiones de impresión , a estas se les conoce como sesión de impresión o bien LU (unidad Lógica) de Impresión, mientras que las LU de DISPLAY son designadas para terminales, los dos tipos de LU por lo regular se definen juntas para un mejor control. Bien en el caso de impresión, Este es muy importante por que la mayoría de las empresas que tienen un MAINFRAME por lo regular tienen que entregar algún tipo de recibo para proporcionarlo a los usuarios de algún servicio.

Estos son solo algunos de los servicios que puede ofrecer algún Mainframe. Y el tratar de administrarlos se vuelve un tanto complicado cuando se presenta un problema, aun para una personas experta. Ya que esta puede resolverla en cuestión de minutos u horas o bine solicitar soporte al gigante azul (ya que es él el único que puede ofrecernos apoyo), pero para entonces transcurrieron mínimo un par de horas. Lo cual representa una gran perdida para la compañía. Ya que esto provocaría una desesperación para el usuario final que se encuentra pagando o consultando algún estado de cuenta, en otras palabras se tendrían grandes filas de personas molestas por no poder realizar sus tramites.

II.4. AREA DE TELEPROCESO.

Esta área fue creada en su momento para atender cualquier problema físico con las comunicaciones incluyendo problemas básicos de rupturas de cableado, daño en equipos de comunicación, desconfiguración de ruteadores, problemas de enlace de líneas privadas o conmutada, caídas de energía , etc. hasta problemas más serios como lo puede ser la caída del sistema, problemas con los cables de canal (cables que inter-conectan en forma serial los equipos controladores nivel 4 con los anfitriones nivel 5).

Lo anterior no solo es problema de una compañía en particular si no que es un problema común de las empresas que crecen aceleradamente y que llegan a un punto en el que los

servicios son insuficientes, y cada ves los usuarios quieren una respuesta mas rápida del sistema así como de sus recursos, esto es se requieren canales de transmisión mas rápidos.

Aunado a esto y el poco personal que algunas compañías se cuenta y personal calificado, es la causa de problemas mas serios , como lo es la caída general de la red.

La caída del sistema no solo afecta a las personas que administran la red sino a la compañía en general ya que por cada equipo de comunicaciones que se encuentre caído, son varias sucursales o centros de atención que las personas que laboran en tales centros de atención les provocan serios problemas, ya que ellos a su vez ofrecen un servicio a un usuario o aun cliente . Por tanto son perdidas importantes y considerables para todos.

II.5. PROCEDIMIENTOS.

Los procedimiento son o bien eran un tanto tediosos ya que para hacer una nueva conexión se requería un lapso de tiempo considerable, debido a que participan otras entidades o departamentos. Como lo son construcción, cableados, instalación de líneas y proveedores de servicio externos a la compañía. Razón por la cual la instalación o conexión de una simple estación o terminal se complicaba. Aunado a esto se encontraba el papeleo reglamentario así como una infinidad de memorándums justificar o apoyando dicha instalación. Aun más si la instalación se trataba de instalación de un servicio en una ciudad del interior de la republica, esto es una sucursal foránea aun más se complicaban las cosas.

Es por ello que son necesarias nuevas técnicas de procedimientos así como metodologías para aminorar tiempos de respuesta en la implantación de nuevas conexiones.

II.6. MANTENIMIENTO.

El mantener una RED de la cual no se tiene documentación normalizada (esto es con una estructura, o una norma); se complican las cosas, ya que al crecer apresuradamente no da tiempo para documentar cada segmento de la red. Es por ello que se vuelve un tanto complicado. Pero se tienen que hacer planos de la estructura de la red, afortunadamente al iniciarse la red se contaban con algunas herramientas , como por ejemplo la red TCP/IP y la red Novell para el primer caso se cuenta con Cisco works , una herramienta que permita administrar y monitorear redes Ethernet, Para el caso de la red Novell Simplemente se agregan servidores a la red y los supervisores de dicho servidor se encargaban de administrarlo, siendo ellos los únicos responsables de la estructura del servidor y aplicaciones instaladas en los mismos. Pero los problemas se complican al meter la red SNA en la red Publica , la pregunta es como se va a dar soporte de algo nuevo para los usuarios que apenas saben dar su USERID y un PASSWORD cuando el sistema se los pide. Bueno pues hasta este momento la red digamos iba creciendo poco a poco siendo un área responsable de dar el servicio y mantenimiento a la red. Como es el caso de administrar

ruteadores, controladores, Getways dar de alta a usuarios dentro de servidores Novell, bajo ambiente Unix tampoco se presentaban problemas ya que los administradores de dichos equipos eran los responsables de administrarlos.

Así que todo recae en la administración como tal de la RED en cuanto a las comunicaciones, ya que cada elemento que la forma es administrada en primera instancia por un administrador caso particular de los servidores Novell , de los equipos con sistema operativo UNIX.

Por tanto el mantenimiento de la red Publica se limita únicamente al medio de transmisión la cual es responsabilidad de esta área la cual se debe de encargar antes de que se presenten los problemas o la caída de enlaces , ruteadores, o equipo de comunicación el solucionar o reparar dicho equipo. Y que se encuentra en optimas condiciones.

En ocasiones surgen problemas como el daño en equipo de comunicación y en tal caso el área no cuenta con equipo de stock para su reparación por tal motivo el tiempo de respuesta es mayor ya que se depende de un proveedor de servicios externo a la compañía. Y en tales caso lo único que queda es levantar un incidente o reporte.

Pero la finalidad de implementar un centro de control es el detectar las fallas antes de que se presenten y tratar de dar mantenimiento a los equipos para que estos no fallen, claro esta en la medida de lo posible.

Otro punto importante es que se cuenta con verdaderos sistemas de Contingencia, esto es a lo mas que se cuenta son con equipos de respaldo de energía (plantas de energía), de Incendios, y de seguridad , pero se contempla muy poco la integridad de la información como es el caso de equipo de comunicación que es muy costoso y que en el se encuentran almacenados grandes cantidades de información o bancos de datos, que con simples comandos se pueden borrar o alterar, es por ello que son necesario niveles de seguridad tanto de acceso como de administración.

Para el caso en que se presenten perdida de información se debe contar con respaldos de información o bien que el centro de control no sea centralizado (esto es que todo se encuentre en un solo lugar) ya que se puede presentar el caso de incendios, desastres naturales o de algún otro tipo que pueda alterar o dañar dichos sistemas. Este punto se explica más a detalle en el siguiente capitulo en planes de contingencia.

II.7. AREA DE MONITOREO.

HERRAMIENTAS DE MONITOREO

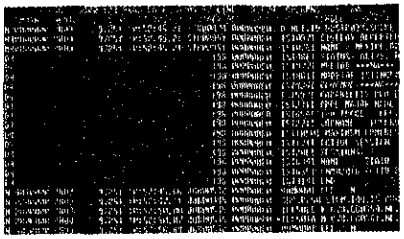
Las herramientas con las que se contaba en un principio era únicamente con una terminal conectándose como un usuario normal y dando comando de sistema operativo de TSO en READY o bien bajo 8.6.log revisar los eventos que se hubiesen presentado a determinada hora, estos eventos son registrados por el sistema todo el tiempo en un archivo. Y que es

utilizado precisamente para observar que sucedió cuando algún equipo se allá dado de baja o bien cuando se salen de sistema las LU's (unidades lógicas). Estos comandos Por lo general igual que un sistema operativo o un lenguaje. Son necesarios se introduzcan al sistema con una sintaxis y en una secuencia para que estos sean ejecutados correctamente.

A continuación se muestra una ventana de comandos bajo el Prompt READY de TSO y una Ventana mostrando parte de la información contenida en el Archivo de eventos Sys. LOG bajo TSO (opción 8.6.log).

```
READY
help commands
 LANGUAGE PROCESSING COMMANDS:
 ASM         INVOKE ASSEMBLER PROMPTER AND ASSEMBLER F COMPILER
 CALC        INVOKE ITF:PL/1 PROCESSOR FOR DESK CALCULATOR MODE
 COBOL       INVOKE COBOL PROMPTER AND ANS COBOL COMPILER.
 FORT        INVOKE FORTRAN PROMPTER AND FORTRAN IV G1 COMPILER

 PROGRAM CONTROL COMMANDS.
 CALL        LOAD AND EXECUTE THE SPECIFIED LOAD MODULE.
 LINK        INVOKE LINK PROMPTER AND LINKAGE EDITOR.
 LOADGO      LOAD AND EXECUTE PROGRAM.
 RUN         COMPILE, LOAD, AND EXECUTE PROGRAM.
 TEST        TEST USER PROGRAM.
 TESTAUTH    TEST APF AUTHORIZED PROGRAMS.

 DATA MANAGEMENT COMMANDS:
 ALLOCATE    ALLOCATE A DATA SET WITH OR WITHOUT AN ATTRIBUTE
             LIST OF DCB PARAMETERS.
 ALTLIB      DEFINE OPTIONAL, USER-LEVEL OR APPLICATION-LEVEL SETS OF

 SESSION CONTROL:
 CONSPROF    DEFINE USER CONSOLE CHARACTERISTICS.
 EXEC        INVOKE COMMAND PROCEDURE.
 EXECUTIL    ALTER REXX ENVIRONMENT
 HELP        INVOKE HELP PROCESSOR.
 LOGOFF      END TERMINAL SESSION.
 LOGON       START TERMINAL SESSION.
 PROFILE     DEFINE USER CHARACTERISTICS
 SEND        SEND MESSAGE TO OPERATOR/USER
 TERMINAL    DEFINE TERMINAL CHARACTERISTICS
 TIME        LOG SESSION USAGE TIME
 TSOEXEC     EXECUTE AN AUTHORIZED OR UNAUTHORIZED COMMAND
             FROM WITHIN AN UNAUTHORIZED ENVIRONMENT.
 WHEN        CONDITIONALLY EXECUTE NEXT COMMAND.

DATA MANAGEMENT COMMANDS

ALLOCATE    ALLOCATE A DATA SET WITH OR WITHOUT AN ATTRIBUTE
            LIST OF DCB PARAMETERS.
ALTLIB      DEFINE OPTIONAL, USER-LEVEL OR APPLICATION-LEVEL SETS OF
            LIBRARIES CONTAINING SAA/PL EXECS OR CLISTS.  THESE
            LIBRARIES ARE SEARCHED WHEN IMPLICITLY INVOKING AN
            SAA/PL EXEC OR CLIST.
ATTRIB      ALLOW DCB PARAMETERS TO BE DYNAMICALLY INTRODUCED
            AND NAMED FOR USE WITH A SUBSEQUENT ALLOCATE COMMAND.
CONVERT     SIFT ITF/PL1 AND FORTRAN SOURCE.
COPY        COPY A DATA SET.  (SEE NOTE BELOW.)
DELETE      DELETE A DATA SET
EDIT        CREATE, EDIT, AND/OR EXECUTE A DATA SET
FORMAT      FORMAT AND PRINT A TEXT DATA SET.  (SEE NOTE BELOW.)
FREE        RELEASE A DATA SET AND/OR AN ATTRIBUTE LIST.
LIST        DISPLAY A DATA SET.  (SEE NOTE BELOW.)
LISTALC     DISPLAY ACTIVE DATA SETS
LISTBC      DISPLAY MESSAGES FROM OPERATOR/USER
LISTCAT     DISPLAY USER CATALOGUED DATA SETS
LISTDS      DISPLAY DATA SET ATTRIBUTES

Un comando tipico es el siguiente:
logon
 SITMFRP LOGGED OFF TSO AT 10:36:45 ON SEPTEMBER 8, 1997
 IKJ56700A ENTER USERID -
sitmfrp
```

La siguiente ventana muestra una ventana bajo una terminal mostrando parte de los eventos suscitados en un determinado momento de un día normal. Esta ventana muestra información de una sesión de una LU=D2STP033, con el siguiente comando /D NET,ID=D2STP033,SCOPE=ALL, como se puede ver el tratar de interpretar las siguientes ventanas es un tanto complicado aun para los operadores.



Como se puede observar el tratar de interpretar todas y cada una de las líneas en las 2 ventanas de información presentadas por la única herramienta llamada NetView , es muy complicada. Esto únicamente para el ambiente de la RED SNA.

Por parte de las otras 2 redes Novell (IPX) y UNIX (TCP/IP) ya se contaba con una herramienta llamadas LAN Analyzer y Cisco Works el cual permite monitorear cada ruteador y ser configurado fácilmente

CAPITULO III. IMPLEMENTACION DE UN CENTRO DE CONTROL.

III.1. ENTORNO E IMPLEMENTACIÓN DE UN CENTRO DE CONTROL Y MONITOREO.

El propósito de implementar un centro de control es con la finalidad de poder administrar y monitorear una red corporativa, para el caso particular de esta tesis se considero que el centro de control debe ser un centro de control con la siguientes características:

- Implementarse a nivel nacional sin perder el dimensionamiento de la red. El dimiensionamiento involucra la red Ethernet, la red (Novell, TCP/IP y la integración de la red SNA con la Ethernet a Través de Tarjeta CIP de) así como la Red Token Ring, la Red FDDI, y la integración de estas a la RPD(red Publica de datos).

- El área Física donde se va implementar debe contar con los requerimientos necesarios de seguridad

En este rubro se tienen que contemplar los siguientes puntos:

Sistemas de seguridad de Acceso Restringido tanto de acceso a áreas físicas y salidas de emergencia.

  - Así como tomar medidas de seguridad de acceso a los sistemas computacionales a través de implementación de niveles de acceso(Claves, Password etc.) contra Hakers.
  - Sistemas de energía como media de seguridad
  - Procedimientos o esquemas de respaldo de información
  - Procedimientos de recuperación de información
  - Planes de contingencia contra desastres en general

- Cableado estructurado, será necesario implementar según norma de cableados como la Systimax para cableado.

- Adquirir software que permita monitorear y administrar la red Corporativa esto incluirá los siguientes protocolos como Ipx, SNA, TCP/IP entre otros , que son los utilizados por esta red.

  - El software será capaz de monitorear y administrar con el mayor lugo de detalle la Red.
  - El monitoreo tiene que ser de preferencia con herramientas gráficas o de fácil utilización capaz de poder crear Script Personalizados para realización de procedimientos o tareas automáticas, simulando un operador lógico
  - Permitir la distribución de archivos de configuración mediante herramientas gráficas.

- Permitir monitorear el ancho de banda utilizado así como el desempeño utilizado por lo recursos del sistema y aplicaciones.
- Personalizar tareas para solución de problemas
- Capacidad para enviar Pagers (mensajes) de activación de alarmas
- Permitir la detección de problemas en línea y solucionarlos en el menor tiempo posible.
- El centro de control no tendrá un esquema centralizado, de presencia dos centros de control a nivel nacional como medida de respaldo en caso de que se presente alguna falla o problema.
- Deberá contar con una administración que permita contar con niveles de atención de llamadas (área de Help Desk) para la atención de problemas.
- Los tiempos de respuesta deberán ser loa más corto posibles

III.2. DIMENSIONAMIENTO.

Como se menciona al principio de este capitulo se tienen que Implementar un dimensionamiento de lo que se quiere administrar y monitorear nivel nacional. El dimensionamiento involucra la red Ethernet, la red (Novell, TCP/IP y la integración de la red SNA con la Ethernet a Través de Tarjeta CIP de) así como la Red Token Ring, la Red FDDI, y la integración de estas a la RPD(red Publica de datos).

A continuación se describe brevemente cada una de las redes así como la forma en que se encuentran interconectadas además de mencionar las principales características y ventajas que presentan cada una. Incluyendo algunos esquemas gráficos de como es que se lleva acabo la integración de todas estas en una sola red llamada red publica de datos.

red ETHERNET

Novell
TCP/IP

Esquema Gráfico
Dimensiones de red Incluir plano de red Novell/IP

red SNA

Esquema Gráfico
La arquitectura de SNA (desarrollada por IBM), es sin duda muy popular, extensamente instalada y una de las más complejas dentro del ambiente de las telecomunicaciones y computación.

Se considera que un porcentaje de aproximadamente de 60 a 70% de todas las redes del mundo están basadas en este tipo de arquitectura. Especialmente en el ambiente financiero, la arquitectura SNA ha ganado importante parte del mercado comparado contra otro tipo de arquitecturas.

A pesar de que el término "arquitectura", nos provee las reglas para el desarrollo de nuevos productos, ésta pueden tener cambios, de acuerdo con el desarrollo técnologico. Sin embargo se pretende que una arquitectura sea independiente de un producto específico de hardware o software y de ahí la importancia desde el punto de vista técnico de SNA.

III.2.1. REFERENCIA DE SNA CON EL MODELO OSI.

Un concepto básico común entre todos los tipos de arquitecturas de redes de comunicación es la división de funciones de red, definidas a través de capas con funciones específicas. A pesar de que SNA fue desarrollada antes que el modelo OSI, podemos hacer en forma muy general una similitud entre las capas de OSI y las capas de SNA para su mejor entendimiento.

La siguiente tabla muestra las principales capas de SNA y su equivalencia en OSI.

SNA	OSI
Aplicación	Aplicación
Manejo de Funciones	Presentaciónn
Control de Flujo de datos	Sesion
Control de Transmisión	Transporte
Control de Ruteo	Red
Enlace de datos	Enlace de datos
Control Físico	Fisica

III.2.2.TERMINOLOGIA COMÚN,UTILIZADA EN SNA.

Dado que SNA es una combinación de hardware y software, es necesario definir algunos elementos especialmente de hardware para comprender el modo en que se construye una red SNA

Mainframe:

Los mainframes, frecuentemente se les denomina "Host" y tradicionalmente es el punto central o corazón de una red de IBM. Todos los procesos que un usuario realiza al teclear su terminal son ejecutados en el Mainframe. Existen una variedad de modelos desde los S/370 a principios de los 70's, pasando por los 43XX, 30XX y recientemente por los modelos 91XX. Los Mainframes, dentro de la terminología de SNA normalmente se denominan como "PU (Physical Unit) Tipo 5".

Controlador de Comunicaciones:

También conocidos como "Front End Processor (FEP)", los cuales son en realidad computadoras de la serie 43XX, que tienen por objeto descargar al MainFrame de todas las tareas de comunicaciones, como es el "poleo" de la "unidades físicas" (PU). Estos controladores pueden ser conectados en cadena para extender las comunicaciones entre MainFrames o tener conectados "Cluster Controllers", que es el siguiente dispositivo de comunicación. Los tipos de FEP's que normalmente se encuentran en el mercado son:

3705	SDLC,BSC	No soportado.
3725	SDLC,BSC,TIPor	ser descontinuado.
3720	SDLC,TIC	Soportado.
3745	DLC,TIC,T3	Soportado.

El software que reside en estos eqipos es el NCP (Network Control Program), el cual define y controla los recursos de la red. Estos dispositivos son denominados como PU Tipo 4

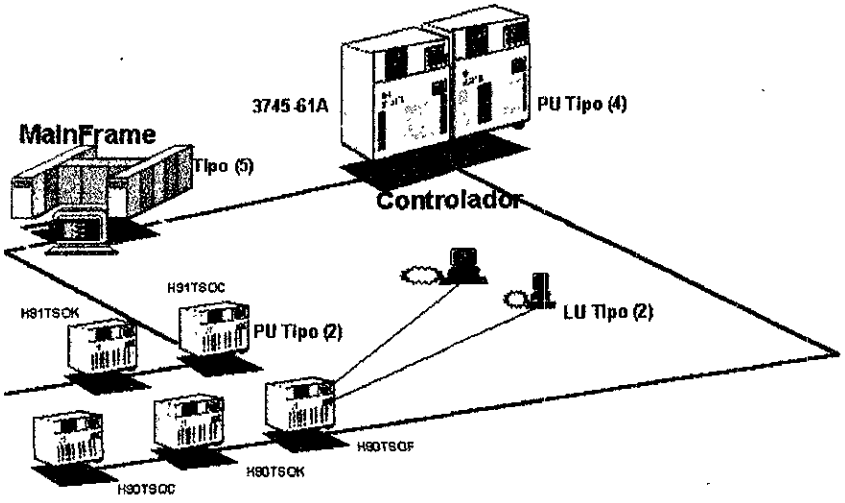
Cluster Controliers:

Tambié denominados Control Units, son máquinas que supervisan y controlan los dispositivos primarios o elementales como las impresoras y tenninales que utilizan los usuarios.

Hay varios modelos de Cluster Controllers como los antiguos 3276 y 3274 que soportan tambien BSC y más comunes los 3174 que ofrecen puertos SDLC y TIC o los nuevos 3172 con puertos SDLC, TIC o Ethemet, los cuales van directamente conectados al Mainframe, en vez de ser conectados al FEP. Al igual que con los dispositivos antes mencionados, los Cluster Controllers son definidos con PU 2.

Terminales. e Impresoras denominadas LU, para lo que las terminales para poder conectarse necesitan emular una terminal 3270 esto es definir el teclado con una configuración especial.

La figura siguiente, muestra una configuración básica de una red SNA. (type 5) que controla la red. Conectada al host está el controlador de comunicaciones (type 4). Hay tres clusters controllers (type 2) conectados al FEP. Los controladores 1174 o 3174 pueden ser conectados en forma local o en forma remota para el primer caso se conectan los controlador es a canal junto con el resto de los equipos, mientras que para el caso de los controladores remotos son necesarios módems o fraccionadores así como líneas privadas o algun medio de transmisión como DS0, Ds1 o E1 o E0. En los controladores se les puede conectar hasta 32 terminales o impresoras.



Tráfico SDLC (synchronous data link control).

Es otro concepto utilizado por las redes SNA., este traafico generado por las sesiones que se establecen entre una aplicación corriendo en el host y un usuario en su terminal. La concentración de tráfico la tenemos en los cluster controllers que pueden soportar hasta 32 dispositivos de usuario (terminales, impresores ete ...) o hasta 64. La conexión entre el cluster y el FEP se hace normalmente utilizando el protocolo SDLC en líneas de baja velocidad 9.6 a 19.2 Kbps. Con el explosivo crecimiento de las LAN'S, las tradicionales terminales han sido desplazadas por PC's y protocolos de comunicación como token ring han permitido aumentar la velocidad de comunicación con los hosts.

Sin embargo, SDLC es en muchas organizaciones el protocolo dominante de su red SNA. El problema principal de este protocolo es su bajo "throughput", debido a que es un protocolo maestro/esclavo que da control completo a la estación primaria sobre la secundaria. En SNA, el FEP es la estación primaria mientras que los cluster controllers son secundarios.

La estación secundaria solo puede enviar información cuando son poleados por el FEP. Cuando no son poleados, no pueden usar la red.

El poleo consume una gran cantidad de ancho de banda del canal, además de crear suficiente retardo en el tiempo de respuesta como para que el performance de la red se degrade o incluso se llegue a dar el caso de cerrar la sesiones de los usuarios.

Es evidente que bajo estas circunstancias, sería ineficiente integrar una red SNA a una red de área amplia (WAN) multiprotocolo. Una de las maneras en se puede realizar esta integración es a través de la utilización de Gateways.

GATEWAYS

Como se mencionó anteriormente, las LAN's han introducido una variedad de protocolos que no es conveniente que viajen a través de las tradicionales líneas SDLC. Afortunadamente, dispositivos como los FEP y los Cluster controllers, han sido parte de la revolución de la era de LAN's y actualmente, muchos de ellos tienen internases de red local como por ejemplo token ring, ethemet, además de sus tradicionales puertos SDLC.

Estas interfaces permiten enviar tráfico SNA a un gran número de estaciones conectadas a la red las cuales pueden utilizar diferentes protocolos como pueden ser Netbios, IPX/SPX, Banyan, TCP/IP, APPLETALK, etc... Existen una gran variedad de tipos de gateways para poder integrar SNA a una red multiprotocolo, los cuales varían de acuerdo al método que utilizan para integrar SNA.

Los métodos más comunes utilizados por los gateways son:

- Conversión de SDLC-LLC2-
- Source Routing Bridging (SRB).
- SNA/IP.
- Gateways propietarios.

CONVERSIÓN DE SDLC-LLC2.

Este tipo de gateways son particularfnente útiles cuando los FEP's cuentan con interfaces de LAN (Token Ping, Ethernet o FDDI), pero los dispositivos remotos o periféricos como los cluster controllers cuentan únicamente con puertos SDLC. Adicionalmentese pretende integrar los servicios de la red SNA a una red multiprotocolo, utilizando un solo enlace de WAN entre la localidad remota y la central. La figura siguiente, muestra una situación como la descrita anteriormente.

SNA/IP

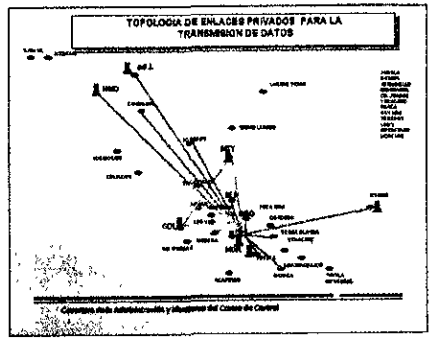
Este tipo de Gateways puede ser aplicado cuando la infraestructura de la red SNA solo tiene puertos SDLC, sin embargo, es necesario integrarla a la red multiprotocolo utilizando únicamente IP como protocolo ruteable a través de los enlaces de WAN. Este escenario es común, dado que TCP/IP, se ha reposicionado en el mercado casi como el estándar de comunicaciones de industria y en muchas organizaciones se ha optando TCP/IP como su protocolo de WAN. Al implementar este tipo de protocolo (IP) como se describirá más adelante en acceso vía CIP(Cico Channel Interface Processor) permite a las redes SNA

interoperar con usuarios que tiene TCP/IP como protocolo, al ver al HOST como un elemento más dentro de la red TCP.

Al igual que con los gateways de conversión SDLC-LLC2, estos gateways realizan un poleo local con los dispositivos SDLC (FEP's, clusters, etc ...), eliminando tráfico a través de] enlace de WAN. La figura siguiente muestra este caso práctico. Los beneficios que se obtienen con esta solución son similares a los de] conversión, más la flexibilidad de poder utilizar TCP/IP y OSPF como protocolo ruteable. Es sin embargo impotante establecer que no es recomendable incluir esta funcionalidad dentro de los equipos de ruteo por el excesivo procesamiento de CPU que se requiere, el cual va en detrimento del performance del ruteador.

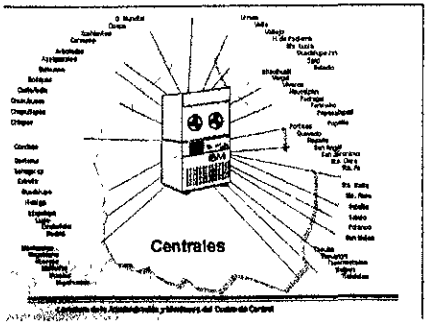
Dentro de un ambiente SNA existen otros conceptos o elementos que interactuan entre si, como son: VTAM(Virtual Telecommunications Access Method), CICS(Customer Information Control System), IMS(Information Manager System), TSO(Time Sharing Option), CMS(Conventional Monitor System), JES2(Job Entry Subs System 2), Emulaciones de terminal que permiten configurar el teclado con un tipo de configuración especial generalmente utilizado por los equipos Mainframes, 5250 Emulación de terminal utilizada por los equipos AS/400 la cual configura el teclado con un tipo de configuración especial que entienden los equipos AS/400. Etc..

La cobertura que tiene que tener el centro de control se muestra en la siguientes laminas, en primera instancia se tiene que monitorear la red a nivel nacional, cubriendo aquellas principales ciudades como Monterrey, Guadalajara, Yucatán, Cd. Juarez entre otras.

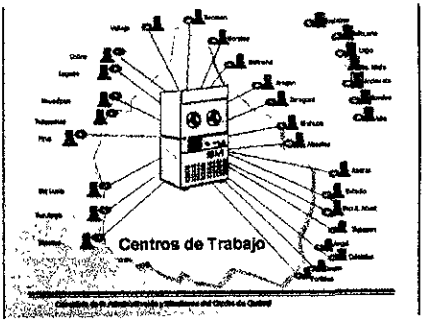


Que proporcionan servicios a terceros, como es el caso de centrales telefónicas, Centros de Trabajo, Comerciales. Que de una u otra forma le dan atención al publico. Y el servicio tiene que ser en línea, No se puede dar el lujo uno de tener caído algún equipo de comunicación o enlace.

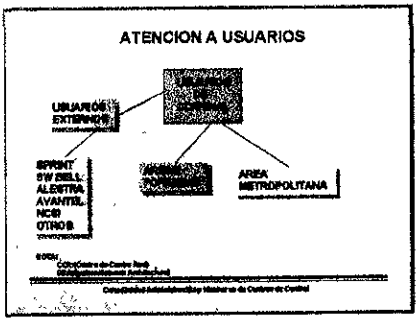
A nivel Distrito federal se tienen que monitorear las centrales telefónicas, que también son parte importante , ya que en estos lugares requieren de consultar la Bases de datos, transmisiones de datos etc.

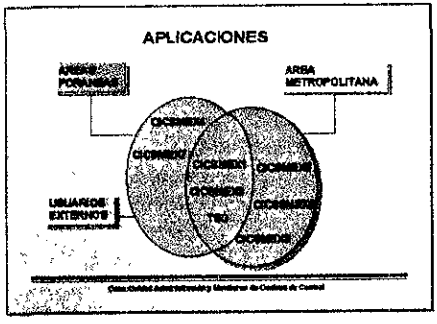


Los centros de trabajo también requieren consultar información en el MainFrame, imprimir sus ordenes de servicio, esto es las rutas de trabajo que van a realizar durante un día etc. Es por ello que es parte esencial las comunicaciones en una empresa ten grande.



También se tienen conexiones con usuarios externos a la empresa como son Avantel, Alestra, Sout Wester Bell,NCSI, Bancos entre otras que rentan o comparte su información con esta compañía.





Como se muestra en las laminas anteriores, la cobertura es bastante amplia a nivel Distrito y a nivel nacional incluso con compañías externas que consultan o que depositan información en el MainFrame, pero no solo son la conexiones lo que importan sino que hay un sin numero de personas que utilizan este medio para consultar información y al mismo tiempo proveer un servicio. Este es el caso de las oficinas comerciales, al no tener servicio de sistema, esto puede volver un caos en cuestión de minutos, pues esto implicaría grandes filas de personas molestas tratando de pagar sus recibos telefónicos

III.2.3. CIP (CHANNEL INTERFACE PROCESSOR).

Como se ha venido comentado en el capitulo anterior anates no se podian interconectar redes disimiles como lo eran las redes Ethernet con ambientes de equipos grandes como lo eran los Mainframnes en una red SNA con su protocolo SDLC. Pero ahora con la implementación de TCP/IP para MVS esto ya es posible. En pocas palabras al inplementarse en un mainframe o equipo minis con TCP/IP estos equipos se convienten en un nodo mas para una red TCP/IP.

Cisco en colaboración con Sterling creador del Netmaster y IBM son los precursores de este ripo de conexión del IOS para el sistemas operativos 390 el cual es un stack de TCPIP para equipos 390 de IBM. ¿Como funciona o que se necesita para implementar e interconectar ambass redes? lo explicare de una forma sencilla. Bien se requieren lo siguiente.

Primero:

Requerimientos

Es necesario el Software TCP/IP que será instalado en el HOST (Mainframe), para ello existen actualmente dos productos el propio de IBM y el TCP/IP de CISCO el cual en base a convenios con IBM, quien le proporciono parte del microcodigo para que desarrollara su propio TCP/IP, estos son el TCP 2.2 MVS/VM , el CISCO IOS vrsion 2.0. cabe señalar que se tienen que hacer algunas definiciones en las tablas de TCP/IP en el Mainframe como La CLAW esto es similar a la MAC adress de una tarjeta de red, para el sistema son necesrios estos datos , por ejemplo la dirección IP que tendra el HOST, el LINK , la IP del HOME entre otros y que no es otra cosa que definir el IOCP.

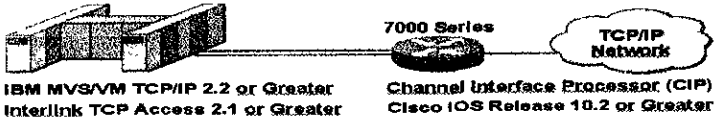
Definicion en el IOCP en MVS
CHPID PATH =06 TYPE=BL CNTLUNIT CUNUMBER=0600,UNIT=3088, PROTOCOL=S4, UNITADD=((E0,8)) IODEVICE ADDRESS=(6E0,8),CUNUMBER=0600, UNIT=CTC

Definicion para Datagramas IP en el Profile de TCP/IP de MVS

```
TCP/IP PROFILES(IPDATAGRAM)
DEVICE CIP1 CCLAW 6E0 HOSTTCP CIPTCP NONE 20 20 4096 4096
        LINK CIP1A IP 0 CI1
      HOME
      <DIRECCION IP>
      GATEWAY
      Network          fist hope              drive   packet size      Subnet  mask    subn
value
        127            =              CIP1A   4096          1.1.255.0                0
DEFAUTTNET 128 207 28.1      CIP1A   1600    0
START CIP1A
```

Estas son solo algunas de las lineas importantes que se tienen que tomar en consideración para ser definidas en el IOCP y el Profile de TCP

En la siguiente gráfica se muestra un Mainframe con su TCP/IP conectado la CIP que se encuentra insertada en un ruteador Cisco serie 7000 y el cisco conectado al Backbun de la Red TCP/IP



Segundo:

Tipo de arquitectura de canal

Se requiere la Interface de procesamiento de Canal (CIP **C**hannel **I**nterface **P**rocessor) y un ruteador de preferencia de la serie 7000 de Cisco donde será colodada la tarjeta CIP. Bien La tarjeta CIP se presenta en dos tipos de arquitectura de canal, para realizar la conexión entre la red Ethernet y la conexión directa al Mainfram. Estos son PARALELO y ESCON(**E**nterprise **S**ystem **CON**nection) en el primer caso es utilizado para la conexión de la CIP directamente a canal y como su nombre lo indica Paralelo se requieren dos cables y es generalmete utilizado donde la distancia entre dispositivos como Mainframe, unidades de respaldo, controladores etc. que se encuentran a corta distancia) para ello se implementa dos tipos de conectores BUS(Canal que transmite las señales de los datos) y TAG(canal que transmite las señales de control). En el segundo caso el tipo de arquitectura ESCON a diferencia de la de tipo paralelo presenta una interface de fibra Óptica. la cual esta formada por un par de conectores RX,TX y en cada extremo de la fibra presenta un transductor (LED,lasser) para transmitir y recibir la señalización a una velocidad aproximada de 200Mbps. y es utilizada cuando se quiere conectar también a canal dispositivos como unidades de respaldo, controladores etc. que se encuentran una distancia considerable, la transmisión en forma de señales luminosas evita la atenuación de la misma, permitiendo así una mayor velocidad y contabilidad.

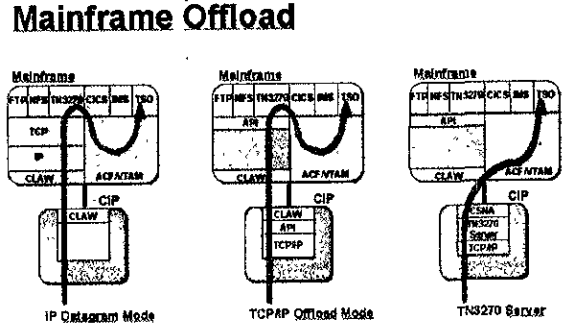
Una vez conectada la tarjeta CIP es necesario configurar el Ruteador donde se encuentra insertada la Tarjeta CIP la cual tiene las siguientes características (permitir el paso de Datagramas, Soporta TCP OFFLOAD, Protocolo SNA y configurar como Servidor TN3270) dependiendo de cómo se quiera habilitar, es como se tiene que configurar. También se tiene que configurar el Ruteador con las siguientes líneas:

Configuración en el ROUTER
Router Config (IP datagram)
Interface channel 0/0
Ip address <direccion IP><mascara>
Ip route Cache cbus
No keepalive
Channel-Protocol s4
Claw[1] <datos de la cip y dirección ip>

Tercero:

El Desempeño es un punto muy importante ya que cada ciclo de procesamiento en un Mainframe es Muy caro, es por ello que es necesario implementar la CIP como OFFLOAD en lugar de DATAGRAMAS IP, en pocas palabras diremos que TCP/IP en el Mainframe realiza el direccionamiento IP de cada dirección asignada a una Unidad lógica(LU) causándole carga al Mainframe por cada ciclo, esto no es muy notorio si se tienen pocos nodos en la red , pero cuando se tiene una red conformada por unos cuantos miles de nodos esto provoca un gasto en cuanto al desempeño de un Mainframe. Para esto existe una par de alternativas una de ella es llamada OFFLOAD este sistema consiste en descargar al Mainframe de la carga de direcionamiento y que lo realice la CIP dejándole al Mainframe el proceso de FTP Server , NFS y emulación de Terminal TN3270.

A Continuación se presenta un comparativo entre el modo OFLOAD y el de DATAGRAMAS IP y la migración de servidor TN3270, según CISCO para la optimización de la CIP.



[1] *Claw es un protocolo de comunicación a nivel de canal de SNA, el cual se tiene que configurar tanto en las tablas de TCP/IP del Mainframe como en el Ruteador.*

En el primer modo el MainFrame es quien realiza el ruteo(direccionamiento TCP/IP) y la CIP deja pasar todo, esto por supuesto genera una carga para el MainFrame, posteriormente sube al siguiente nivel para realiza un (FTP,NFS,TN3270,CICS,MS o TSO) estableciéndose la conexión.

En el segundo caso la idea es descargar de ciclos de procesamiento en el MainFrame (direccionamiento IP), pasándole el trabajo a la CIP, para dejar al MainFrame el servicio de FTP,NFS,TN3270. TSO.

Existe una tercera forma de configurar este sistema, la cual implica que además de quitarle carga de trabajo al Mainframe (direccionamiento IP), También quitarle la función de servidor de terminal TN3270, esto es como se muestra en los dos casos anteriores es necesario pasar primero por una emulación de terminal, para posteriormente entablar una sesión bajo TSO. En esta ultima opción la idea es que la CIP Funcione como un GATEWAY haciendo la función intermedia de Servidor de Terminales 3270. Para dejarle únicamente al MainFrame la conexión a TSO.

Cuarto:

La Seguridad y respaldo

Existen dos formas para implementar las seguridad la cual se enfoca la utilización de redundancia usando un protocolo llamado RIP(Routing Information Protocol, Protocolo de información de Ruteo, utilizado para determinar un número de saltos e informar a los ruteadores si cambio alguna ruta) y redundancia con VIPA(Virtual IP Addressing, Direccionamiento virtual de IP) es un concepto implementado por IBM para redundancia la cual se explicara a continuación.

Las presentes las dos gráficas anteriores muestran un comparativo entre la utilización de redundancia utilizando RIP y utilizando VIPA, en el caso del RIP lo realiza el Ruteador intermedio el cual como se muestra antes y después que se presenta una caída de una Ruta este debe ser capaz de resolver y encontrar o más bien desviar el trafico por una ruta alterna, previamente definida como ruta estática en el Ruteador, cabe señalar que se requiere como medida de respaldo el utilizar dos tarjetas CIP. El Mainframe en este caso HOST sele tiene que definir algunos parámetros en una tabla llamada PROFILE que se encuentra en librería TCPIP.V3R1.PROD(PROFILE) la cual es la librería que se encarga de cargar el TCPIP en el MainFrame, algunos de estos parámetros son definir un HOME, rutas estáticas, definir dos direcciones una que funcionara como dirección primaria y la otra como dirección secundaria.

Para el caso de la implementación de VIPA, se requiere también hacer algunos cambios en la tabla llamada PROFILE que se encuentra en librería TCPIP.V3R1.PROD(PROFILE) y considerar que se va a utilizar Ruteo Dinámico (RouteD). ¿Cómo funciona? Bueno. La idea principal es que se asigna una dirección virtual en el Mainframe, esto es una dirección intermedia que no esta asociada a una tarjeta de red física(MAC Address).

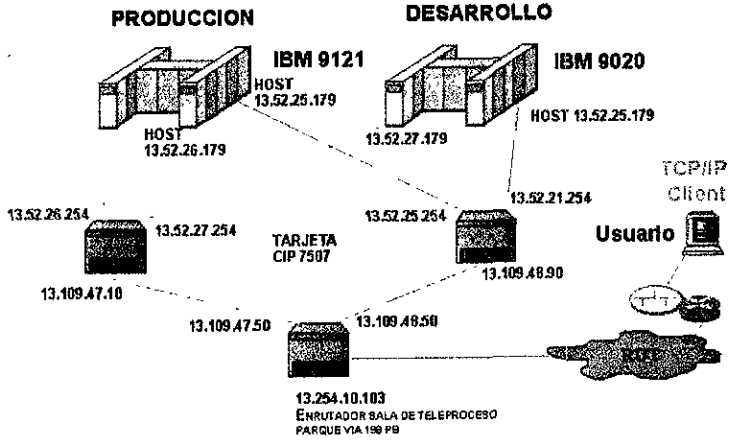
Y observando la gráfica se puede explicar mejor, cuando se presenta una caída física de uno de los dos ruteadores lo qu hace el tercer ruteador es buscar una ruta alterna hacia la

dirección virtual la cual a su vez apunta a el HOST, en pocas palabras significa que si un usuario quiere entablar una sesión 3270 con el Mainframe para el va ser transparente ya que únicamente tendrá que apuntar hacia la dirección virtual y la dirección virtual se encargara de resolver por donde llegar al HOST

La presenta gráfica muestra como se encuentra conectado actualmente la CIP y los dos Mainframes con los que se cuentan en México (Desarrollo y Producción) implementados con TCP/IP

Se tiene implementado el esquema de Datagramas utilizando RIP como Redundancia, para ello se cuenta con 3 ruteadores dos de ellos que se encuentran cruzados con las dos máquinas (Desarrollo y Producción) utilizando una tarjeta CIP en cada uno, de tal forma que si se presenta algún problema con alguna ruta se pueda tener acceso por la ruta alterna. Pasando por un tercer ruteador que se encuentra físicamente conectado entre los dos ruteadores y la red publica de datos (RPD).

Existe otra forma un poco mas drástica pero funcional cuando se presente un problema en algún segmento entre los ruteadores intermedios que contienen las CIP, el cual consiste en cambiar el cable que se conecta a canal (cables Azules) BUS y TAG de una CIP a la otra CIP , posteriormente entrar como administrador al ruteador que se encuentra funcionando y cambiar la dirección IP por la dirección IP del que no se encuentra funcionando y listo se tiene otra vez sistema. Mientras se checa cual fue el problema que causo la caída de la otra ruta, la cual puede se un cable un ruteador o la propia CIP que falle. Pero mientras eso sucede ya se puede contar con sistema.



Beneficios de utilizar una CIP permite empaquetar el protocolo de SNA sobre TCP/IP

- Se puede reducir la carga de trabajo en el Mainframe
- Puede extenderce una red SNA sobre una red TCP/IP utilizando anchos de banda más grandes como FDDI, ATM y FAST Ethernet

- Se puede monitorear utilizando agentes SNMP
- Se puede también administrar bajo NETVIEW
- Bajo costo en cuanto al MIB al implementar la CIP como un servidor TN3270

III.3. RED TOKEN-RING.

Es una tecnología LAN sofisticada avalada por IBM y definida por el estándar IEEE802.5. Token Ring utiliza una topología de cable de estrella en la cual todas la estaciones de trabajo se conectan a una unidad de acceso multi-estación (MAU). Esto hace que el movimiento, cambio y adición de equipo sean hechos con rapidez y facilidad.
Es también tolerante a las averías. Si por ejemplo, el cable de una de las computadoras personales en la red esta dañado o cortado, el MAU automáticamente desviara ese acceso. Puesto que el anillo lógico permanece intacto, por tanto la red no se detiene.

Es también fácil de conectar a una unidad principal(Pu tipo 4). Esto es que se puede interconectar directamente la red Token Ring a un controlador IBM 3174 (en la cual podría ser necesaria una estación de trabajo)

LA topología de red Token Ring ofrece alta velocidad del rango de 16Mbps. Y puede conectar hasta 72 dispositivos utilizando cable par trenzado sin proteger (categoría 3,4 o 5) o hasta 260 dispositivos utilizando par trenzado Protegido.

Red FDDI
Como parte de la red (cableados estructurado)

III.4. AREA FÍSICA.

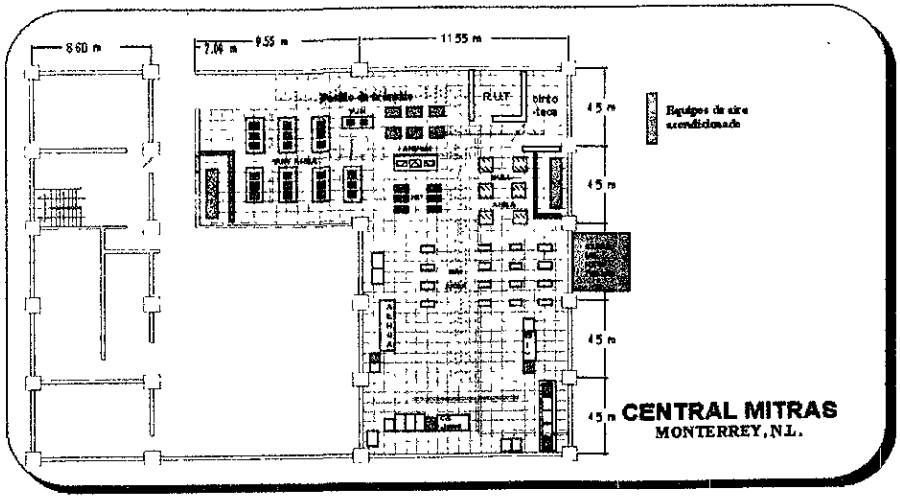
- El área Física donde se va implementar, debe contar con los requerimientos necesarios de seguridad

En este rubro se tienen que contemplar los siguientes puntos:

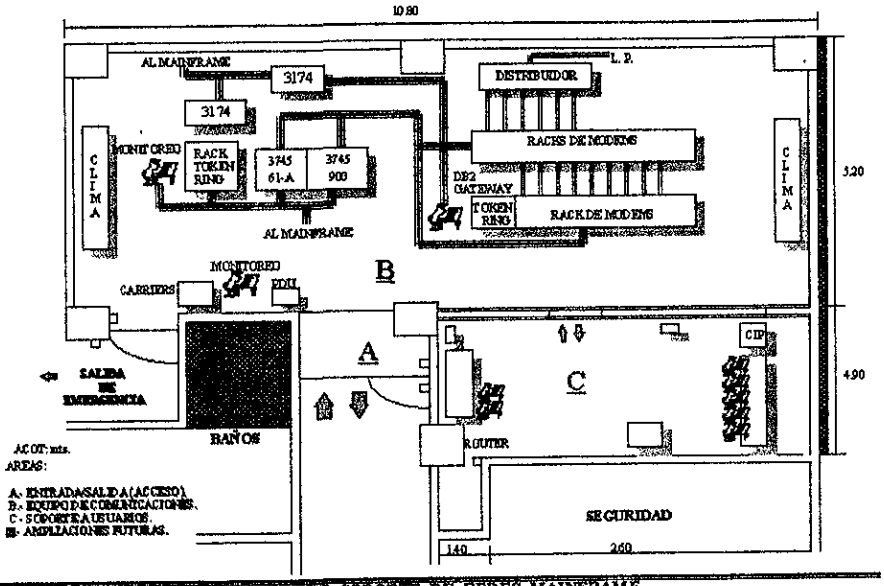
Sistemas de seguridad de Acceso Restringido tanto de acceso a áreas físicas y salidas de emergencia.

- Así como tomar medidas de seguridad de acceso a los sistemas computacionales a través de implementación de niveles de acceso(Claves, Password etc.) contra Hakers.
- Sistemas de energía como media de seguridad
- Procedimientos o esquemas de respaldo de información
- Procedimientos de recuperación de información Planes de contingencia contra desastres en general

Plano de Distribución e Implementación centro de Control



Centro de Control México



PLANO DE UBICACIÓN DEL AREA DE SOPORTE DE REDES MAINFRAME.

III.5. CABLEADO ESTRUCTURADO.

SISTIMAXs un sistema que muestra los aspectos principales de un cableado estructurado. Existen varios documentos que establecen los parámetros a seguir para la adecuada implementación de un cableado estructurado.

Los Elementos Principales de un Cableado Estructurado se pueden clasificar en los siguientes:

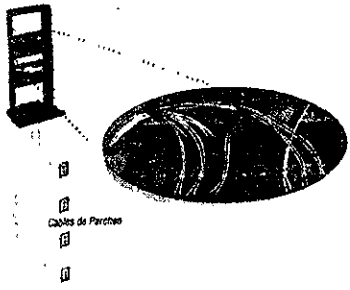
Cableado Horizontal; El cableado horizontal (cajas/placas/conectores) incorpora el sistema de cableado que se extiende desde la salida de área de trabajo de telecomunicaciones (Work Area Outlet, WAO) hasta el cuarto de telecomunicaciones.

Los costos en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal pueden ser muy altos. Para evitar estos costos, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario. La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la relocalización de áreas de trabajo.

El cableado horizontal deberá diseñarse para ser capaz de manejar diversas aplicaciones de usuario incluyendo:

- Comunicaciones de voz (teléfono).
- Comunicaciones de datos.
- Redes de área local.

El diseñador también debe considerar incorporar otros sistemas de información del edificio (por ej. otros sistemas tales como televisión por cable, control ambiental, seguridad, audio, alarmas y sonido) al seleccionar y diseñar el cableado horizontal.



Cableado del Backbone; El propósito del Cableado del Backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en

edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

Cuarto de Telecomunicaciones; Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de Telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que puedan haber en un edificio.

- Ejemplo de racks combinando cableado estructurado y servidores.
- Ejemplo de racks combinando teléfono y datos.

Cuarto de Equipo; El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de vídeo. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo. Los requerimientos del cuarto de equipo se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569 que hacen referencia a Rutas, Espacios de Telecomunicaciones y Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

Cuarto de Entrada de Servicios; El cuarto de entrada de servicios consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto o espacio de entrada. El cuarto de entrada puede incorporar el "backbone" que conecta a otros edificios en situaciones de campus. Los requerimientos de los cuartos de entrada se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

Documentación Adicional y estándares que definen un cableado estructurado son descritos a continuación con más detalle:

SYSTEMAX® Descripción general del sistema de cableado estructurado

Sistema de distribución para instalaciones

Un sistema de distribución para instalaciones es la red de transmisión en el interior de un edificio o en un campus de edificios. En el sistema, los elementos de comunicación de voz y datos, dispositivos de vídeo y automatización de oficinas, equipo de conmutación y otros

equipos de gestión de información están conectados entre sí y con redes de comunicación externas. El sistema incluye todo el cableado y los componentes de distribución relacionados, entre el punto donde el cableado del edificio se conecta a la red exterior o a las líneas de la compañía telefónica, y las terminales de voz, datos y vídeo en los centros de trabajo. El sistema también puede dar servicio a un edificio o a grupos de edificios en instalaciones de tipo campus. Un sistema de distribución consiste en varias familias de componentes, incluyendo medios de transmisión, equipo de gestión de circuitos, conectores, jacks, clavijas, adaptadores, circuitos electrónicos para transmisión, dispositivos de protección eléctrica y equipo de apoyo. Estos componentes se utilizan para construir subsistemas de propósito específico que permiten una implantación sencilla y transiciones sin problemas a mejoras en la tecnología de distribución cuando cambian los requisitos de comunicaciones. Un sistema bien diseñado es independiente del equipo al cual da servicio y es capaz de interconectar dispositivos diferentes, incluyendo terminales de datos, teléfonos analógicos y digitales, computadoras personales o centrales, o bien equipo común del sistema.

El sistema de cableado estructurado (SCS)

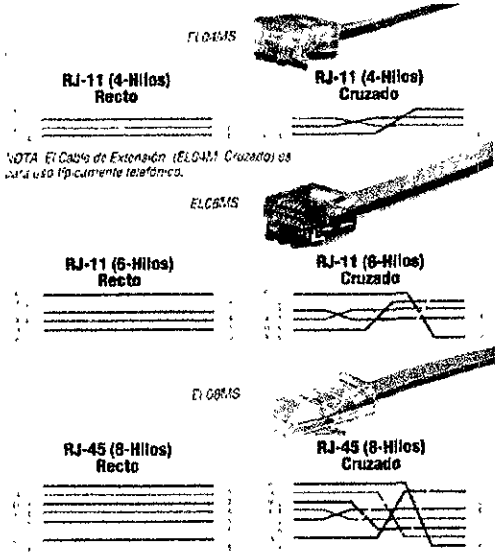
Un sistema de cableado estructurado es un conjunto de productos de cableado y conectividad dispuestos de acuerdo con reglas específicas de diseño de ingeniería. Mejora un sistema de distribución para instalaciones y consiste en lo siguiente:

- Arquitectura abierta
- Medios y disposición estandarizados
- Interfaces de conexión estandarizados
- Cumplimiento de los estándares nacionales e internacionales
- Diseño e instalación de sistema total

SYSTIMAX SCS, de Lucent Technologies

SYSTIMAX SCS es el sistema de cableado estructurado de calidad superior desarrollado por Bell Laboratories, la rama de investigación y desarrollo de Lucent Technologies. SYSTIMAX SCS es una solución avanzada e integrada para redes de cables de fibra óptica o de cobre de par trenzado no blindado que permite el uso sin obstáculos y en forma simultánea de diversas aplicaciones, incluyendo voz, datos, vídeo y control de edificios. Lucent Technologies provee todos los componentes utilizados en SYSTIMAX, incluyendo cable de cobre y fibra óptica. Este factor es de suma importancia, ya que los organismos normativos no dejan de investigar los protocolos multimedia y para redes locales (LAN) de alta velocidad. Llegará un momento en el que será necesario pasar del cableado de cobre a la fibra óptica y las transmisiones inalámbricas. Una compañía estará más tranquila al saber que cuando llegue ese momento sólo tendrá que realizar pocos cambios a un bajo costo. SYSTIMAX SCS es modular y ha sido diseñado teniendo en cuenta el crecimiento y el reacomodo. Usa la topología de estrella de Lucent Technologies, la misma topología física creada por AT&T y la industria telefónica y adoptada por la Norma de Edificios Comerciales EIA/TIA 568A. El crecimiento en una topología de estrella es muy sencilla, ya que las estaciones se agregan hacia afuera desde un punto central. Cada enlace es independiente de

los demás, de manera que los cambios y reacomodos sólo afectan a los enlaces sujetos a cambios. Con esta topología se simplifican la resolución de problemas y el mantenimiento, ya que los fallos pueden localizarse y los informes de dichos problemas pueden centralizarse. La configuración de estrella es versátil, ya que permite una reconfiguración sencilla a otras topologías si así lo requieren las aplicaciones. Si usted mantiene su equipo y cableado en una disposición de estrella, podrá integrar otras topologías con sólo ajustar los circuitos en los puntos de gestión.



La topología de estrella permite que SYSTIMAX SCS tenga un exclusivo enfoque de subsistemas. Con SYSTIMAX SCS, uno puede diseñar una sistema de distribución total que, de hecho, esté formado por subsistemas distintos:

- Backbone o campus entre edificios
- Backbone o vertical en edificios
- Gestión
- Horizontal
- Area de trabajo
- Equipo

Al igual que todos los enlaces de la topología de estrella, cada subsistema es una unidad discreta y los cambios en un subsistema no afectan a los demás. Un ejemplo sería un cambio en el subsistema backbone o vertical de un edificio, reemplazando el cableado de cobre por fibra óptica para aumentar el ancho de banda. En este caso, podría seguir utilizando los subsistemas horizontal, de equipo y de gestión con cableado de cobre en conjunto con la fibra óptica.

SYSTIMAX SCS: Arquitectura abierta

Las soluciones SYSTIMAX SCS se implantan con una plataforma de arquitectura abierta que asegura la máxima conectividad para los productos existentes, a la vez que sirve como el cimiento para una evolución sin problemas a las nuevas tecnologías, como multimedia y ATM (modalidad de transferencia asincrónica).

SYSTIMAX SCS: Medios y disposición estandarizados

SYSTIMAX SCS usa medios estándar, tanto de cobre como de fibra óptica, en cada uno de los subsistemas. En el caso de medios de cobre, la opción disponible es el par trenzado sin blindaje (UTP). Hay dos grados de cables UTP: Categoría 3, para voz y algunas redes locales de poca anchura de banda; y Categoría 5, para redes locales de mayor velocidad y aplicaciones con mayor ancho de banda, hasta 622 Mb/s. Para medios de fibra óptica, la opción es el cable de fibra óptica de guía de luz con núcleo de 62,5 micras. El cable unimodo de guía de luz con núcleo de 8,3 micras puede utilizarse en los subsistemas vertical y entre edificios para aplicaciones con mayor ancho de banda.

SYSTIMAX SCS: Interfaces de conexión estándar

SYSTIMAX SCS tiene interfaces de conexión estándar, tanto de cobre como de fibra óptica, para cada uno de los subsistemas. En el caso del cobre, los paneles de interconexión y de jacks se instalan de acuerdo con la clasificación de categoría del medio: Categoría 3 para anchos de banda hasta 16 MHz y Categoría 5 para velocidades de hasta 622 Mb/s. Lo mismo se hace con las salidas de información en las áreas de trabajo. En el caso de la fibra óptica, los paneles de conmutación y los tipos de conectores de guía de luz se instalan de acuerdo con la ubicación, el tipo de fibra y la cantidad.

SYSTIMAX SCS: Cumplimiento de los estándares

SYSTIMAX SCS ha sido líder en la promoción de estándares y AT&T/Lucent Technologies fue una pieza clave en la formación del Estándar para Cableado de Telecomunicaciones en Edificios Comerciales, EIA/TIA 568. Representantes de Bell Laboratories forman parte de todos los organismos y foros normativos reconocidos que en la actualidad producen los estándares. Entre los cuales se cuentan los siguientes: ANSI (Instituto Nacional de Normas de estados Unidos), la TIA (Asociación de la Industria de las Telecomunicaciones), la EIA (Asociación de la Industria Eléctrica), el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), el Foro ATM (Modalidad de Transferencia Asincrónica), la ISO (Organización Internacional de Normas), la CSA (Asociación Canadiense de Normas) y la AS (Normas Australianas), por sólo mencionar algunos.

Nuevos avances

El estándar actual para edificios comerciales se basa en requisitos mínimos a nivel de los componentes pero no contempla la conectividad entre los componentes. El resultado de esta situación es un estándar que incluye especificaciones de rendimiento mínimo para los componentes individuales. SYSTIMAX SCS, por otra parte, contempla el sistema como un

todo y trabaja en forma constante con el afán de mejorar los márgenes de atenuación, diafonía, pérdida de retorno estructural y equivalencia de impudencias a nivel de los enlaces o canales. Esto es necesario para cumplir con los requisitos de las nuevas redes locales de alta velocidad y las aplicaciones de uso intensivo de ancho de banda, al mismo tiempo que se mejora la tasa de errores en bits (BER) de las aplicaciones actuales.

En épocas anteriores, cuando las velocidades de las redes locales eran de 1, 4, 10 ó 16 Mb/s, se presentaban pocos problemas al aplicar la estrategia de componentes individuales o de nivel de sistema. Esto ha cambiado con la llegada de las redes locales de alta velocidad, de unos 100 ó 155 Mb/s. Como ejemplo tenemos el estándar del IEEE para 100BASE-T4. Este estándar utiliza esquemas de transmisión paralela (un requisito para la transmisión de datos por dos o más pares). Se descubrió que no todos los cables y conectores eran capaces de manejar este estándar. La TIA está trabajando en nuevas especificaciones de oblicuidad por retardo, equilibrio e impedancia para resolver esta deficiencia. Cuando los miembros den el visto bueno, las especificaciones serán añadidas al estándar. SYSTIMAX SCS ya había considerado este asunto y por lo tanto no tiene problemas de retardos de propagación ni de oblicuidad por retardo. Los cables SYSTIMAX Categoría 5 tienen un amplio margen para las redes de alta velocidad, tanto existentes como nuevas.

Esta ha sido la pauta para la reingeniería de la red UTP efectuada por SYSTIMAX SCS. El resultado es un "Estándar de Excelencia de Canal" que ha implantado mejoras considerables, como las siguientes:

- Rendimiento ATM certificado a 622 Mb/s
- Rendimiento superior de diafonía PowerSum
- Apoyo para video de banda ancha a 550 MHz
- Opción de expansión SYSTIMAX SCS

Rendimiento ATM certificado a 622 Mb/s

SYSTIMAX SCS ha estudiado el comportamiento de la transmisión a 622 Mb/s usando cable UTP de Categoría 5. En 1994, Bell Laboratories escribió un artículo y construyó una unidad de demostración para probar de manera definitiva que la transmisión a 622 Mb/s con tecnología 64 CAP opera de manera eficiente en el cableado UTP Categoría 5 de SYSTIMAX. Los estudios de Bell Laboratories serán compartidos con el Foro ATM como parte del proceso evolutivo de la especificación para 622 Mb/s. SYSTIMAX SCS apoya su rendimiento con el Programa de Garantía de Aplicaciones por 15 años para ATM a 622 Mb/s.

Rendimiento de diafonía (NEXT) PowerSum

SYSTIMAX SCS aplica requisitos más estrictos a los cables con alto número de pares destinados a usarse en aplicaciones avanzadas de forro compartido. Al aplicar la tecnología PowerSum al cableado de 4 pares se obtiene un producto con características de rendimiento superiores, ideal para las exigencias de las aplicaciones de alta velocidad que están surgiendo y que vendrán en el futuro. PowerSum está incorporado en los estándares EIA/TIA 568A e

IS 11801. La especificación PowerSum establece un límite de potencia para la interferencia NEXT de fuentes de perturbación múltiples (pares activados en el forro del cable), una configuración típica del cable backbone.

Aunque los comités de estándares apenas han comenzado a estudiar el tema de los forros compartidos, Bell Laboratories probó y calificó la compatibilidad de las redes locales más rápidas disponibles. Las redes token ring de 16 Mb/s par trenzado dependiente del medio físico (TP-PMD) a 100 Mb/s y ATM a 155 Mb/s son compatibles y están garantizadas si se siguen las pautas de SYSTIMAX SCS. Además, el cableado de 25 pares quedó calificado como opción para cableado de zona horizontal. Tenga presente que los productos indicados a continuación están garantizados para cumplir con la especificación PowerSum:

- Salida de comunicación de información MPS-100
- Hardware de distribución Patchmax™
- Sistema de panel de conmutación 110
- Cables LAN de alto rendimiento 1061+ y 2061+, de 4 pares
- Cordones de impedancia equilibrada 1074

Video de banda ancha a 550 MHz

SYSTIMAX SCS ha diseñado un adaptador de video 384A para aplicaciones de banda ancha, el cual ha superado las pruebas de emisión radiada de acuerdo con los reglamentos de la FCC, Parte 76. SYSTIMAX SCS proveerá la garantía de aplicaciones para 77 canales de video de banda ancha (canal 2 a canal 78, intervalo de frecuencias de 55 a 550 MHz) si el diseño cumple con lo indicado en la guía de aplicaciones de video de SYSTIMAX. Esta aplicación utiliza cable UTP Categoría 5.

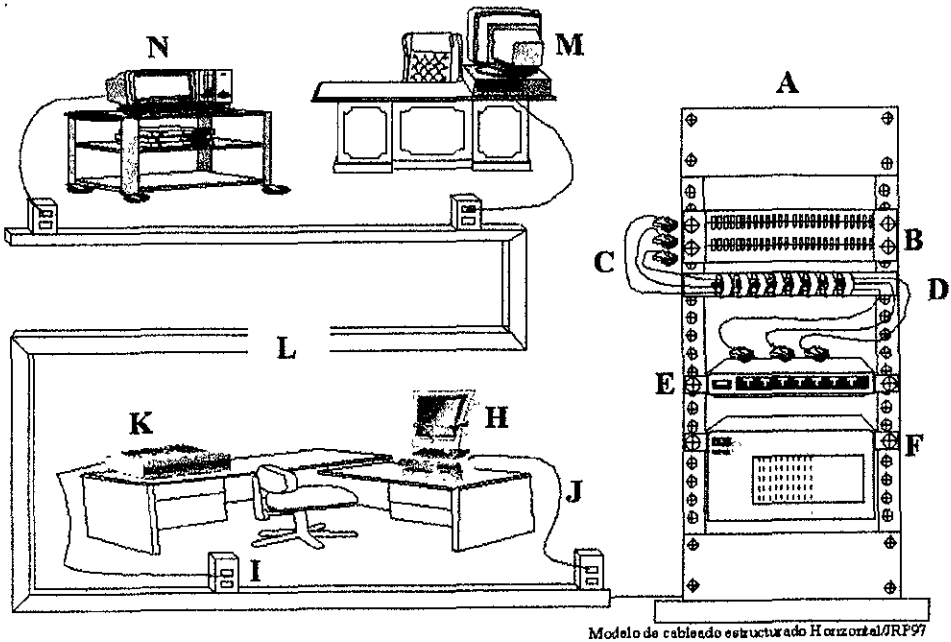
Opción de expansión SYSTIMAX SCS

Esta opción de cableado sirve para apoyar las actividades de movimientos y cambios. Lucent Technologies garantizará el compartimiento de sistemas de datos de alta velocidad calificados en un enlace o canal de cable de 4 ó 25 pares usando productos calificados mejorados (PowerSum). Las pautas de SYSTIMAX SCS especifican opciones para cumplir ologies

Cuatro niveles de asistencia técnica

El tiempo de inactividad del sistema muchas veces se desprecia, considerándolo como un "costo oculto" de la operación. SYSTIMAX SCS puede reducir su tiempo de inactividad entre un 50% y en 80%. La respuesta a la pregunta "¿Cómo?" es muy breve: con calidad. Las pruebas están certificadas. Cada uno de los componentes empleados en SYSTIMAX (cobre, fibra óptica, sistemas inalámbricos, incluso el equipo de conectividad) se fabrica de acuerdo con estándares de control de calidad tan estrictos que incluso exceden las especificaciones ISO-9001. Los científicos e ingenieros de los Laboratorios Bell trabajan para alcanzar esta meta.

El siguiente dibujo muestra el tipo de Modelo de cableado horizontal implementado en cada uno de los pisos del edificio donde se encuentra el centro de control de monitoreo de redes, describiendo parte por parte los elementos que lo forman, según lo marca el modelo de cableado estructurado de SystiMax.



Modelo de cableado estructurado Horizontal/JRP97

Modelo de cableado implementado en el centro de control de red

A).-RACK
B).- Pach Panel
C).- Patch cord con conectores RJ45
D).- Sujetador /Ordenador de Cableado
E).- Concentrador (HUB)
F).- Equipo de comunicaciones (Ruteador, Bridge, GateWay, Puente etc.)
H).- Equipo PC con tarjeta de RED
I) - Roseta para pared plástica
J).- Patch Cord
K).- Nodo Impresora con tarjeta de Red Interna
L).- Canaleta Plástica Superficial (PANDUIT)
M).- Nodo Estación de trabajo con tarjeta de RED
N).- Nodo tipo Terminal con Tarjeta de Red.

III.6. MONITOREO.

A medida que una red crezca, sus necesidades de administración cambiaran, lo cual llegara un momento en que ya no será posible administrar dicha red, por tal motivo será necesario implementar sistemas que puedan adaptarse a los cambios y que permitan tener un control total de los dispositivos o componentes que integran una red, como son Ruteadores, Hub's, Getways etc. que enlazan a los usuarios dentro de una red

Otra necesidad es la de poder administrar desde un solo punto central (desde una sola estación) y resolver cualquier tipo de problema de comunicación que se presente en la red, desde un control sencillo de una red LAN hasta la planificación y diseño de redes complejas de manera que uno pueda expandir su red LAN o WAN de una manera ordenada. Sin que se cause una baja de desempeño en la red. Todo esto suena muy bien pero actualmente no existe un producto que pueda realizar dicha labor debido a que la red de la que estamos hablando es una red corporativa la cual incluye redes disimiles que en su momento no se podian administrar con un solo producto y desde un punto central debido a la complejidad de la misma, estas redes como se menciona al principio de este capitulo son: redes LAN (IPX Novell), TCP/IP y SNA, FDDI, TOKEN RING y en algunos caso X.25.

En el presente capitulo se describen brevemente algunos productos que actualmente se están utilizando como herramientas para la administración y monitoreo de redes así como sus características y sus principales ventajas que presentan , así como su facilidad de instalación y utilización entre otros.

III.6.1. ADMINISTRACION.

Actualmente se pueden administrar las redes utilizando algunos protocolos que permiten de manera más fácil y amigable el monitoreo de las mismas. Pero ,¿Que Software o que producto es mejor para ser utilizado como herramienta de administrar en un centro de control, esta sería la pregunta, pero desafortunadamente no se puede responder con una sola herramienta debido a que no la hay, y para poder implementar dicha herramienta se deben considerar algunos aspectos en la misma antes de adquirirla.

Según las necesidades y magnitud de la red que se quiera administrar o monitorear. Dichos aspectos son los siguientes:

1. Permitir el monitoreo a través de recolección de agentes SNMP
2. Tener interfaces amigables con el operador (Ambiente Gráfico)
3. Debe ser capas de descubrir rutas(estáticas y en algunos casos rutas dinámicas)
4. Debe ser capas de poder monitorear el mayor número de protocolos (TCP/IP. IPX,RIP, PPP,ARP,HDLC, entre otros
5. Debe permitir monitorear el ancho de banda de determinados canales
6. Permitir monitorar Protocolos ruteables

7. Crear archivos que permitan generar estadísticas

III.6.2. HERRAMIENTAS DE MONITOREO Y ADMINISTRACIÓN.

A continuación se describen Brevemente los requerimientos y las principales cualidades que presentan los siguientes productos que permiten el monitoreo de redes:

Agentes SNMP

Antes de mencionar las cualidades que presentan tales productos mencionaremos como es que funcionan estos utilizando algo llamado agentes SNMP.

Que es un agente SNMP

El SNMP trabaja a través de tres comandos, estos requieren solamente de servicios de transporte básicos por lo que es un protocolo independiente. Esto significa que la información en SNMP se puede intercambiar con casi cualquier protocolo de red local.

Componentes del SNMP:

- Agente
- Administrador
- Base de información para la administración (MIB Management Information Base)

El agente es compatible con SNMP residente en el software de la red, dispositivo inteligente como los concentradores, ruteadores, puentes o tarjetas de interfase (NIC, network interface card), es capaz de monitorear las tareas de la estructura de comunicaciones, colectando datos acerca de su ambiente, aún de aquellos procesos sofisticados.

¿Que es un agente apoderado?

Los dispositivos que no soportan un agente SNMP deben manejarse con un agente apoderado, este tiene la misma función que el agente pero al mismo tiempo sirve como convertidor de protocolo. Convierte los comandos del SNMP en instrucciones que pueden ser comprendidas por el dispositivo propietario y viceversa.

¿Como interactuan los administradores y agentes?

El agente responde a las peticiones del administrador para proveer información específica acerca de los periféricos. Para un concentrador, podría ser el número de paquetes recibidos o el número de veces que un puerto ha sido particionado. El administrador también puede solicitar ciertos datos ambientales, como el IP del dispositivo o que se cambie el nombre asignado a un puerto específico. Por último el administrador también puede solicitarle al agente que controle las comunicaciones, por ejemplo que active o desactive un puerto. El

administrador reacciona a las alarmas de los agentes, por ejemplo un mensaje intermitente cuando un hub se ha accionado o un puerto ha sido particionado.

¿Que ha sido monitoreado y controlado?

Asociado con cada enlace de comunicación, hay una serie de recursos que pueden ser controlados y monitoreados. Estos recursos, o variables, definen la personalidad de los periféricos. El conjunto de recursos constituye el MIB (Management Information Base).

¿Que es el MIB y donde reside?

MIB es la base de datos en el marco de SNMP, contiene un conjunto estándar de variables que es soportado por los agentes y administradores. Dos ejemplos de variables estándar son la dirección de los dispositivos y el número de paquetes IP transmitidos. El MIB también contiene los recursos específicos del proveedor. Estos son aumentados por el proveedor para mejorar el manejo de sus propios productos.

El MIB reside en cada agente o administrador de la red. Cada agente, para ser realmente compatible con SNMP, debe contener un conjunto mínimo de los recursos estándar de MIB así como **las** variables específicas del proveedor. Así mismo cada administrador debe tener un depósito del MIB, una colección del MIB representando cada uno de los dispositivos en la red, el administrador usará la información de los dispositivos almacenada en el MIB para entender la información que recibe de los agentes.

La introducción de los nuevos productos basados en SNMP, trajo una proliferación de nuevos MIB'S. Para controlar esta situación se han formado comités para desarrollar estándares para la creación de MIB en los diferentes tipos de productos. Este esfuerzo toma validez con la formación del Repetidor IEEE 802.3 MIB, que identifica los recursos administrables en un repetidor Ethernet.

¿Como se comunican los administradores y agentes de comunicacion?

Cualquier tipo de comunicación requiere de un vocabulario común y de un uso gramático definido para ese vocabulario. El MIB, tanto el que reside en el agente como en el administrador, provee el vocabulario y el SNMP la gramática, juntos definen como se intercambiarán los mensajes.

El SNMP es comúnmente referido a un protocolo de estímulo-respuesta, para cada solicitud emite una respuesta. Hay tres verbos básicos en su conjunto de comandos: Get, Set y Trap. Al usar el comando "GetRequest" el administrador le solicita la información al agente, este le manda la información necesaria con un comando de "GetResponse".

El administrador deberá usar el comando de "SetRequest" para controlar el dispositivo cambiando el valor de una de las variables del MIB. Así, el agente responde con el comando de "GetResponse". El "SetRequest" no es soportado por todos los proveedores, algunos lo soportan únicamente por un número limitado de variables. Si no se usa con cuidado el comando Set puede afectar las operaciones de la red.

El agente también alerta al administrador, vía el comando "Trap" cuando encuentra algún problema (por ejemplo un puerto particionado) y entonces el administrador liberará una alarma.

Los mensajes de "Get", "Set" y "Trap" se manejan entre el administrador y los agentes, a través de un protocolo de transporte. Como el SNMP es un protocolo independiente, puede usar cualquier vehículo de paquete.

La gran mayoría de los concentradores inteligentes van acompañados de una internase gráfica de software, que nos permitirá desplegar de una manera gráfica, la información que provean los concentradores.

El software de administración podrá utilizar la información recolectada del concentrador para diagnosticar, predecir y controlar el tráfico en la red.

La gran mayoría del software de administración, necesitan de una plataforma de administración que sirva de enlace entre el hardware (Concentradores) y la interfase gráfica (Software de Administración) como el SunNet Manager, HP OpenView, IBM NetView, Novell NMS(Novel] Management Services)

CiscoWorks

Cisco Works Es una serie de aplicaciones que utilizan agentes SNMP para manejar los dispositivos que se encuentran conectados en una red. Este producto puede implementarse en diferentes plataformas y diferentes sistemas operativos, Cisco Works lo componen una serie de aplicaciones que permiten administrar una red por ejemplo entre otros

Aplicación	**Dispositivos que pueden ser Administrados**	**Plataformas Requeridas**
Cisco Works	Permite administrar diversos dispositivos Cisco	SunNet Manager Hp Open View con HP-UX IBM Netview para AIX
Cisco Works Blue MAP	Ruteadores con la bandera habilitada de SNA	SunNet Manager Hp Open View con HP-UX IBM Netview para AIX
Cisco Works Blue SNA View	Ruteadores con habilitación de SNA y dispositivos SNA manejados por un Mainframe	SunNet Manager Hp Open View con HP-UX IBM Netview para AIX
Cisco Works Blue Native Services Point	Permite monitorear y administrar Ruteadores Cisco	IBM Netview para MVS Netmaster
Cisco Works Windows	Permite administrar ruteadores, Swiches, concentradores, Servidores de Accesoswiches Atm y otros adaptadores.	SunNet Manager HP-Open View con Sun Os/Solaris Hp Open View con HP-UX IBM Netview para AIX
Cisco View	Permite administrar ruteadores, Swiches, concentradores, Servidores de Accesoswiches Atm y otros adaptadores	SunNet Manager HP-Open View con Sun Os/Solaris Hp Open View con HP-UX IBM Netview para AIX

¿Que puede hacer CiscoWorks?

Auto Instalación

Es una herramienta que le permite a Cisco Works remotamente instalar y configurar a un nuevo ruteador en la red utilizando la configuración de algún otro que se encuentre también en la red. Esto es que no se requiere que se realice la configuración manualmente, ya que los ruteadores vecinos detectaran el nuevo ruteador y le informaran del segmento y ruteadores que se encuentran en sus limites para que se auto configure.

Cisco View

Permite Proveer el estado, estadísticas y la configuración necesaria a otros dispositivos que se encuentran en la red tales como (ruteadores, swiches, servidores de acceso, concentradores y Adaptadores). Así como registrar y mostrar gráficamente en la estación que se encuentra monitoreando toda la información recolectada.

Cisco Network Management Support CD-ROM

Contiene las ultimas actualizaciones de archivos de soporte, estos archivos son organizados en el producto en forma de paquetes y enviados a los dispositivos que requieran de actualización. Con la Implementación de ayua en CD le permite mostrar información detallada de los dispositivos, mostrando incluso vistas de los conectores que se encuentran en los ruteadoress.

Configuración de archivos

Herramienta que permite tener un mejor control en la administración de ruteadores o dispositivos de lar red que utilizan agentes SNMP, Esto es nos permite saber que administrador o usuario entro al dispositivo. Así como saber que cambios realizado.

Contactos

Herramienta que permite personalizar los ruteadores con información de personas a las cuales se pueden contactar para solicitar ayuda, esta herramienta le da infamación como números telefónicos, direcciones de correo electrónico etc.

Manejo de Dispositivos

Herramienta que permite tener, crear y mantener una base de datos que contenga un completo inventario de Hardware Software y asociarlos con nombres o localidades físicas donde se encuentren.

Comandos Globales

Es una facilidad que le permite al administrador de la red crear archivos de configuración genéricos que serán enviados a diferentes ruteadores con las mismas características de una manera rápida y sencilla. Esto evita que se configure dispositivo por dispositivo.

Análisis de RED Fuera de Línea

Esta es otra de las herramientas importantes de administración ya que permite capturar tramas de un momento determinado en la red y capturarlas como variables de agentes SNMP y posteriormente crear archivos de bases de datos y posteriormente generar gráficas.

Administración de Seguridad

Permite también tener una mejor seguridad en la red ya que se puede habilitar en cada dispositivo el acceso restringido, esto es que se pueden crear grupos de administradores los cuales solo mediante el uso de su usuario y password podrán entrar y realizar modificaciones en los equipos de comunicaciones. Lo cual evitara a algún tipo de persona y por error realizar algún cambio.

Los Puntos anteriores son algunas de las cualidades y características que presenta Cisco Works como soluciones a la administración y monitoreo de redes

Cisco Works puede implementarse sobre la siguiente arquitecturas y ambientes operativos y para ello son necesarias la siguientes especificaciones :

CiscoWorks para HP Open View (HP-UX)	
Descripción	**Especificaciones**
Requerimientos de Hardware	SistemaHP-9000 serie 700 o 800 500Mb de espacio libre en Disco 64 Mb en memoria RAM 128 Mb de espacio para Swap Unidad de CD ROM Monitor Color
Requerimientos de software	HP-UX A:09.04 a A 09 05, 10 01 HP OpenView 3 3 (para A.09.X1), 4.01,4.1

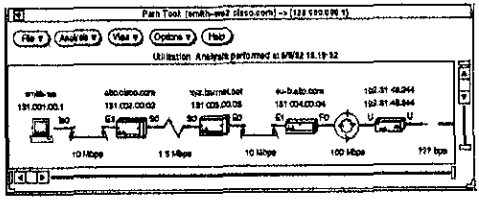
CiscoWorks para HP Open View (SUNOS/Solaris)	
Descripción	**Especificaciones**
Requerimientos de Hardware	Sistema SUN SPARC Station 500Mb de espacio libre en Disco 64 Mb en memoria RAM 128 Mb de espacio para Swap Unidad de CD ROM Monitor Color
Requerimientos de software	HP OpenView 3 3, 4 01, 4.1 SUNOS4 1 3 o Solaris 2.4, 2.5

CiscoWorks para SUNNet Manager	
Descripción	**Especificaciones**
Requerimientos de Hardware	Sistema SUN SPARC Station 400Mb de espacio libre en Disco 64 Mb en memoria RAM 128 Mb de espacio para Swap Unidad de CD ROM Monitor Color
Requerimientos de software	Sun[2] Net Manager 2.3 Sun OS 4.1.3 (Solaris 1 x/SunOS 4.1.4) Solaris[3] 2.4, 2.5

CiscoWorks Blue MAPS/Blue SNA View

Tanto el cisco BLUE MAP como el BLUE SNA VIEW Son dos módulos que son solicitados por pedido al proveedor, estos dos módulos son cargados en el Cisco Works y la función que realizan por ejemplo el BLUE MAP es proporcionar una interface gráfica con el operador de cisco Works al mostrarle mapas de la Red. Mientras que el SNA VIEW proporciona una herramienta también que permite mostrar la estructura de la red SNA en forma de Mapas, los cuales pueden ser controlados por esta herramienta, mostrando algunos menús o ventanas que permiten administrar esta red. Incluso se puede tener control sobre los dispositivos y la unidades físicas, las unidades lógicas. Todo esto entablando una conexión con una LU 6.2 (unidad lógica 6.2), la cual esta informando constantemente del estado de los nodos y las conexiones que se tienen con el MainFrame. Cabe señalar que esto lo realiza de forma dinámica.

A continuación se muestran y describen brevemente algunas pantallas de Cisco Works que presentan infotmación estadística y gráfica de la red.



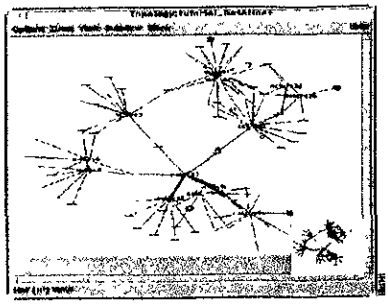
Rutas 1

La siguiente vista muestra información de las rutas y el ancho de banda que se esta utilizando por dicha ruta.

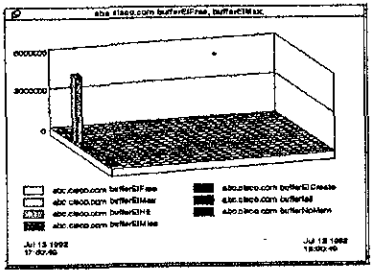
[2] *Es el creador del El software Network File System (NFS - Sistema de archivo en red) de Sun, que permite la utilización comun de datos a través de la red, el cual se ha convertido en un estándar industrial*

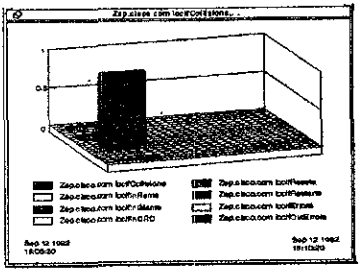
[3] *Solaris:Es un sistema operativo multitarea para computadoras SPARC y PC's de Sun Soft Inc. se ha diseñado para computadoras distribuidas, el cual incluye el protocolo TCP/IP*

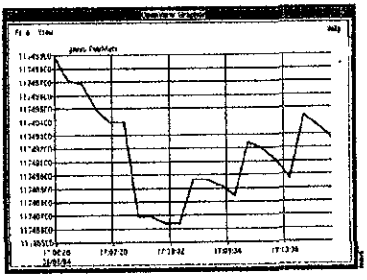
Esta imagen muestra gráficamente la topología de la red, así como cada uno de los elementos que conforman la red. Una ventaja que tiene es que uno se puede ir introduciendo a cada segmento dentro de red y los sistemas nos muestra nuevas vistas de ese segmento, con solo dar un click en el Mouse.



Las presentes tres imágenes muestran información gráfica del uso de algunos recurso, la primera indica el uso de Buffers, en la segunda información del número de colisiones que se han presentado en un periodo de tiempo, mientras que en la última se muestra el número de paquetes que han circulado por algún determinado segmento de red. Estas son solo algunas vistas de las herramientas que utiliza Cisco Work, pero tiene muchas otras.







III.6.3. SUNNET/OPENVIEW.

SNA Blue Point
Netview

NetView es un grupo de programas de supervisión y control de red para redes SNA creado por IBM. El cual controla dispositivos SNA como también no SNA y no IBM, y provee control central sobre la red. NetView/PC es un producto que interconecta NetView con redes de área local Token Ring, Rolm CBXs y modems que no son de IBM, en tanto mantiene el control en el ordenador principal.

NetMaster

Es un conjunto de herramientas para administrar el TCP/IP de Un Mainframe

Netview 6000

Netview 6000 es una aplicación desarrollada e implementada por IBM la cual consiste en presentar la versión de Netview (conjunto de pequeños programas encargados de monitorear una red SNA) bajo ambiente gráfico solo esta nueva versión como el numero 6000 lo indica esta desarrollada para equipos RISC 6000 de IBM. Adicionalmente además de agregar funciones de monitoreo de eventos en la red SNA también lo realiza en la red TCCP/IP. Esto es una aplicación que se instala y configura en una maquina RSIC 6000. Con una arquitectura cliente servidor en donde el servidor es el HOST (Mainframe) y el cliente es el equipo RISC el cual estará registrando los eventos suscitados en la red y lo más sobresaliente de este producto es que muestra los eventos en forma gráfica en el monitor, de tal forma que se puede visualizar los eventos con diferentes tonalidades de colores los cuales indicaran según el color el Grado de problema que presenta un evento, como ejemplo el color verde indica que se encuentra estable un dispositivo, mientras que un color amarillo indica una alarma preventiva, cuando se presenta objetos en color rojo indican que los dispositivos se encuentran con un problema más serio.

Otra cualidad de este producto es que permite enviar mensajes a localizadores personales atreves de algún servicio de radio localización, informando que se presento alguna alarma.

Otra función aun más interesante es la que permite crear administradores automáticos, este concepto indica que cuando el operador o administrador humano no se encuentre en las instalaciones para relizar alguna acción para resolver el problema, el operador automático tomará la decisión de realizar alguna acción (ejecución de Comandos como cerrar archivos, generar respaldos, bajar o subir cintas etc.) en forma automática.

Requerimientos de Hardware y Software

RISC 6000	Mainnframe
Netview 6000	TCP/IP para MVS V3R"
Espacio necesario en HDD 400MB	Definicion de Una LU 6.2
120 Mb en RAM	Netview
Ambiente gráfico OpenView	
Suficiente espacio en HDD también para SWAAP	

Spectrum

SPECTRUM de CABLETROM, la nueva versión 3.0 del software SNMP Spectrum para ambientes cliente /servidor permite administrar 4,000 usuarios dentro de un área de 20 km. Con solo 4 administradores de red. Permite reservar la red para el trafico de datos en vez de sobre cargarla con estadística administrativas . Así mismo. Posee la capacidad de determinar si una falla o falla de actualización es inminente y así detectarla antes de que ocurra. Spectrum 3.0 es una plataforma distribuida que ofrece varias ventajas en su desempeño , entre ella integración "sin costuras" entre bases de datos , lo que permite recuperar información estadística desde cualquier modulo remoto de administración virtual. Spectrum administra todos y cada uno de los dispositivos de la LAN . La configuración básica incluye el motor modelador Spectrucm Server y el software para clientes Spectrum Graph, el cual despliega la información dentro de un ambiente gráfico XWindows o OSF Motif.

III.6.4. MONITOREO Y OFRECIMIENTO DE SERVICIOS A TERCEROS.

Desafortunadamente hay dos situaciones en la era electrónica, las utilidades no pueden proporcionar siempre la alimentación limpia y consistente que se requiere por la sensibilidad de los electrónicos, los clientes son finalmente los responsables por la seguridad y funcionamiento del equipo.

Un estudio de IBM' mostró que una computadora típica está sujeta a más de 120 problemas de alimentación por mes. Los efectos de estos problemas varían desde un simple mal funcionamiento del teclado, degradación del software, a lo más dramático, como la pérdida total de los datos o que la tarjeta madre se queme. De acuerdo a encuestas realizadas por Yankee Group, casi la mitad de las compañías que participaron

Es claro ver que los negocios están aferrándose más a las utilidades de alimentación, las cuales se usan más allá de su capacidad. A pesar de los avances en estas capacidades con las computadoras modernas, el hecho de que se pierda la electricidad momentáneamente, también hace que se pierda la información. Más peligroso aun es la pérdida de archivos que fueron hechos con anterioridad, o inclusive todo el disco duro, lo cual puede suceder si ocurre un problema cuando su computadora esta tratando de guardar un archivo. Los

servidores de archivos Network escriben en el disco constantemente y por lo tanto. Se pueden presentar picos de alimentación o sobrecargas en la red por varios recursos.

Los estándares de Ethernet IEEE 802.3 listan cuatro problemas técnicos a los cuales las redes son susceptibles:

1- Contacto directo entre los componentes de la red local y los circuitos de alimentación o de luces.
2- Almacenamiento de carga estática en los cables de red local y sus componentes;
3- Transición de alta energía, al sistema de cableado de la red local (aquellos inducidos por otros cables que son instalados cerca de los cables de las redes).
4- Diferencia entre las bases de seguridad en la cual se conectan varios componentes de las redes (tales como diferencias que se pueden encontrar en estas bases que van de un edificio a otro).

Seguridad

Como se menciono en el capitulo anterior se necesitan herramienta para implementar la seguridad para evitar que se produzcan caídas de sistema, perdida de información o que puedan entrar usuarios indeseables al sistema. Es por ello que es necesario que se implementen sistemas de seguridad como los siguientes:

Acceso A determinadas áreas, este termino involucra que se tienen que implementar sistemas de seguridad de acceso a determinadas áreas físicas, esto es restringir el acceso solo a usuarios que sean autorizados. Implementando algunos de los siguientes sistemas para un centro de control:

Cámaras de Vídeo o circuitos cerrado de Televisión , existen en el mercado una gran variedad de sistemas de televisión o de circuitos cerrados así como compañías que los pueden instalar e implementar. Estos sistemas incluyen cámaras con movimiento de 360° de giro y movimientos verticales. Además de contar con televisores que pueden presentar hasta 8 (ocho) imágenes en pantalla. Este tipo de sistema permite tener control sobre el personal que entra a el área restringida así como poder visualizar si se presenta algún tipo de evento o bien que se allá activado alguna alarma. Una ventaja de poder utilizar este tipo de tecnología es que se puede grabar las 24 horas del día y poder revisar la información posteriormente para algún tipo de auditoria.

Controles de Acceso, Los controles de acceso en sus inicios solo se valían de un simple portero

Personal de Vigilancia. Es un recurso humano que es necesario ya que siempre la presencia de un policía intimida a las personas a realizar algún tipo de agresión en contra de las instalaciones, además serian las personas responsables de la vigilancia. Entre otras funciones que realizara, está la de control de acceso, el de vigilar las cámaras de vídeo, y llevar una bitácora de eventos, así como hacer rondines de inspección a las instalaciones.

Bitácora de eventos diarios: El personal de vigilancia es quien realizara esta función la cual consiste en llevar un registro del personal interno o externo que entre a las instalaciones.

Existirá una segunda bitácora para los operadores del centro de monitoreo y control donde anotaran los sucesos que se presentaron durante el día y Anotar los procesos que realizaron para resolverlos, o si se quedo abierto algún reporte, de ser así lo deberá informar por escrito.

Todos estos tipos de sistemas se pueden implementar, dependiendo del nivel de seguridad que se necesite será el tipo de esquema que se deberá emplear. Pero lo más importante de implementar algún tipo de sistema de seguridad es tomar la decisión de que se tiene que implementar. Además de ser necesario el involucrar a otras áreas de la compañía para que formen parte en grupos de discusión para que a su vez proporcionen más ideas y ver en que les puede afectar o beneficiar la seguridad para formar nuevas políticas de seguridad.

CAPITULO IV. BENEFICIOS QUE SE OBTIENEN AL IMPLEMENTAR UN CENTRO DE CONTROL.

Permite tener procedimientos de auditoria, esto es saber que administradores o usuarios entraron a realizar modificaciones en los ruteadores o equipo de comunicaciones, así como saber fecha y hora así como los cambios que se realizaron etc.

Soluciones de Administración Completas

- Instalación basada en Windows para una configuración rápida.
- Capacidades completas para la administración basadas en SUMP
- A partir de un solo sistema para redes Cisco de pequeñas a medianas'
- Ofrece, en tiempo real, gráficos de estadísticas, de dispositivos, puertos y red
- Así como mapeo codificado por colores y sistema de alarma para diagnosticar, Identificar y solucionar fácilmente los problemas.
- Compatible con Mm sistemas de administración de sistemas y dispositivos SNMP.
- Adapte las soluciones de administración basándose en la actividad de su red para obtener mayor flexibilidad y eficiencia.
- El instalador de dispositivo de Incremento permite a los usuarios agregar soporte de manejo en base a las necesidades.

Con la diversidad de redes Que existe hoy en día, usted necesita una herramienta de administración completa que funcione con todo el equipo de su red. CiscoWork Windows 2.1 para Windows NR'195 le proporciona las capacidades de administración que necesita para controlar todas las configuraciones de sus routers, conmutadores y servidores de acceso. Controle y superase toda su red con un tablero de administración, desde un solo punto. Las pantallas gráficas codificadas por colores le permiten supervisar y registrar el estado de cada producto a través de la red, y usted obtiene actualizaciones instantáneas del estado de los puertos, de la utilización de amplitud de banda, las estadísticas de tráfico y la información de los protocolos.

Puede adaptar CiscoWork a manera de satisfacer sus necesidades individuales de administración y para automatizar tareas, establecer valores limites de rendimiento y condensar información específica en tablas fáciles de usar. La Base de datos de información administrativa (MIB) Permite manejar cualquier dispositivo SNMP de la red.

También permite utilizar el constructor de configuración para crear y distribuir archivos de configuración mediante herramientas gráficas en lugar de una serie de comandos complicados.

Beneficios de MAP y de SNA View

Permite desplegar información de las unidades físicas (PU) unidades lógicas (LU) y otros dispositivos conectados al MainFrame.

Beneficos :

Reducción en cuanto a costo ya que se puede implementar en una simple consola monitoreando diversos protocolos a diferencia de otros que se requiere un solo equipo por cada protocolo que se desee monitorear.

Incrementa en cuanto a beneficio la administración ya que permite monitorear rápidamente la red SNA. Además es fácil de utilizar.

Otra ventaja que presenta es que permite solucionar problemas rápidamente. Ya puede informar o anunciar mensajes de alerta antes de que se presenten los problemas serios. Permitiendo así dar un tiempo de respuesta inmediato.

Presenta una interface gráfica y sencilla ya que permite mediante ventanas e iconos la representación de los nodos, Links(LNK), Unidades Físicas(PU), Unidades Lógicas(LU) y otros elementos que conforman la red SNA.

A continuación se muestra una tabla con las principales caracteristicas, funciones y beneficios que Cisco Works presenta en su producto Blue SNA View

Características	Descripción /comentarios	Beneficios
Mapa	SNA View le agrega nuevas funciones para la administración de PU y LU Mapas para red APPN Mapas RSRB Mapas DLSw	Determinación de problemas en forma *rápida y sencilla.* Administración desde una sola consola tanto red IP como SNA
Control SNA	- Permite ver el status de las sesiones SNA(PU, LU) - Permite operar desde una workstation con UNIX comandos SNA. - Permite activar y desactivar PU's y LU's Permite encolar y forzar sesiones.	Permite identificar problemas de conectividad Permite administrar y tener control sobre la red SNA desde una *emulación* de terminal bajo una estación de trabajo con Unix.
Manejo de Alertas	Muestra mensajes de alerta antes de que se presenten los problemas.	Permite tomar medidas de prevención antes de que se presenten los problemas.
Integración con plataformas que manejen Agentes SNMP	Para la implementacion de esta servicio son necesarios el Netview de IBM para el sistema operativo AIX Open View de HP o bien el SunNet Manager	Permite interactuar diferentes ambientes de red siempre y cuando utilicen agentes SNMP, una utilidad de esto es que se pueden levantar rápidamente inventarios de equipo que se encuentran conectados en la red, así como administrarla.
Interface Gráfica	Permite administrar más fácilmente al manipular los mapas y encontrar rápidamente *algún dispositivo dentro de la red*	Permite la simplificación de tareas Permite disminuir los tiempos de búsqueda de algún dispositivo dentro de la red.

CAPITULO V. ALTERNATIVAS DE NUEVAS TECNOLOGIAS PARA LA CONEXIÓN, ADMINISTRACION Y MONITOREO DE REDES

V.1. ALTERNATIVAS DE IMPLANTACION DE NUEVAS TECNOLOGIAS.

V.1.1. INTERCONEXION DE REDES WAN.

FDDI

Principales características de las fibras ópticas:

Una baja atenuación por Km. cuando se transmite por las llamadas ventanas de transmisión, que están ubicadas en torno a los valores siguientes de longitud de onda: 0.8 mm, 1.3 mm y 1.55mm. Esta última ventana es la que presenta menor atenuación Total inmunidad al ruido y a las interferencias electromagnéticas, lo que constituye un medio especialmente útil en ambientes con alto ruido. Uso de potencias del orden de los mW, en comparación con otros medios de comunicaciones que requieren potencias mayores. Su pequeño tamaño y poco peso, hacen de ellas medios de comunicaciones fáciles de instalar, especialmente cuando se trata de completar sistemas sobre ductos preexistentes, sobrecargados por otro tipo de medios que no es posible eliminar.

Teniendo en cuenta el modo de propagación, las fibras ópticas se califican en :

Monomodo: Las dimensiones del núcleo son comparables a la longitud de onda de la luz, por lo cual hay un solo modo de propagación y no existe dispersión.

Multimodo: Contiene varios modos de propagación y ocurre en consecuencia al efecto de dispersión. A su vez estas últimas se subdividen en:

V.1.2. ACCESO REMOTO.

Acceso remoto (servidor de acceso remoto) es un nuevo concepto dentro de las redes esto implica

Shiva Lan Rober Es una compañía que sé a dedicado a la creación de dispositivos que permitan conectar ausuarios remotos, esto es que no tienen la posibilidad de accesar una red Ethernet a 10mbs. Y que sus requerimientos son de poder conectarse como usuarios locales a una red.

Esta compañía es una de las primeras en crear este tipo de dispositivos llamado servidor de acceso remoto, el cual permite conectar a usuarios remotos vía una línea conmutada o privada a una red Ethernet o Token-Ring, el dispositivo cuenta con Modems internos de

28000 baudios, el Software que incluye este producto permite configurar, monitorear y administrar la Red, permitiendo crear listas de acceso de usuarios, manejo de seguridad.

Cabe señalar que con dos de estos dispositivos permite conectar dos o más redes que se encuentran separadas formando una sola red. De tal forma que usuarios de un segmento de red pueden ver los servidores del otro segmento de red y viceversa, incluyendo redes TCP/IP

También se puede mencionar que actualmente existen solo algunas compañías que ofrecen este tipo de dispositivos, pero basados en el de Shiva. Como es el caso de IBM quien se alío con esta compañía distribuyendo sus producto pero con el logo de IBM, caso particular con el dispositivo llamado 8235IBM.

Requerimientos de Hardware y Software

Windows requiere una computadora con procesador 386, 486, o Pentium o compatible con IBM PC corriendo Windows Versión 3.1 Software, o Windows for Workgroups 3.11. en 386 y modo extendido. Es recomendable se use 486 o Pentium y mouse.

Para correr el software de instalación y administración sobre un ambiente IPX, es necesario instalar en la computadora controladores ODI para Novell (IPXODI). El Shiva LAN/8235IBM requieren de los siguientes controladores para funcionar correctamente, no es necesario tener un servidor Novell para su implementación.

- LSL.COM Versión 2.05 o superior
- IPXODI.COM Versión 2.11 o superior
- NETX.EXE Versión 3.32 o superior
- VLM Versión 1.10 o superior

Si se quiere implementar bajo un ambiente TCP/IP que es el caso particular de Telmex se requiere configurar el equipo donde se va a instalar con W95 configurar el stack de TCP/IP y asignar un POLL de direcciones de acceso.

Dial BAKC

Este tipo de dispositivos permiten también ofrecer servicios denominado Dial BAK, este concepto implica lo siguiente cuando un usuario remoto se encuentra en una área donde el servicio de telefonía no es local y requiere conectarse a una red, el dispositivo le permite conectarse y posteriormente este ultimo le cuelga y le llama al número telefónico donde el usuario origino la llamada. Esto es muy practico por que no siempre se puede pagar las llamadas de larga distancia, y esto facilita el que el usuario notenga que desenbolsar en pagos de larga distancia. Ya que al colgarle el servidor de acceso remoto y posteriormente hacer la llamada a donde se encuentra el usuario generando una llamada desde la compañía.

Dial OUT

Es otra cualidad que tiene este tipo de dispositivo el cual consiste en permitir a usuarios de una red local que no tiene módem en sus computadoras compartir el servidor de comunicaciones como un módem virtual, esto es que aunque no tiene físicamente el módem en su computadora el usuario puede conectarse al servidor de comunicaciones y de ahí salir a exterior a otros sistemas o bien al la RED de INTERNET.

Como Funciona

En la gráfica siguiente se muestra un esquema de como se encuentra conectado:

1. Supongamos que se planea conectar a un grupo de usuarios que se encuentran en un lugar remoto (su casa, oficina, hotel, avión etc) esto es un lugar que no tiene acceso a la red interna de la compañía pero que requieren de realizar en algún servidor depositar información, correr algún proceso en el Mainframe(caso particular del área de soporte a redes que requiere de dar soporte en línea a usuarios y que solo hay que dar algunos comandos en el Mainframe y no puede en desplazarse hasta las instalaciones de la compañía para realizar esta función).

2. Bien como segundo paso se tiene que conectar el dispositivo de acceso remoto, configurarlo, asignándole una dirección IP, una mascara (255.255.25.0), el ruteador por donde va a entrar o salir los paquetes y el pool de direcciones que este dispositivo va asignar a los usuarios que se van a conectar, Así como si como configurar los protocolos que este dispositivo va a dejar pasar (IPX, TCP/IP, Netbeui, AplleTalk), y configurar si es un dispositivo Ethernet o Token Ring. Asi como configurar rutas estáticas o dinámicas o si va a permitir el Dial Back entre otros parámetros.

3. Explicando la gráfica diremos que el usuario remoto quiere conectarse, bueno primero debe tener el software adecuado o bien si tiene w95 utilizar la herramienta de Acceso remoto, conectar y configurar su módem, conectarse a una línea telefónica conmutada o privada, configurar el TCP/IP de su Pc si quiere asignar una IP o el servidor le asigna una dinámicamente, marcar el número o números telefónicos que le permitirán realizar la conexión con el servidor de acceso remoto.

4. Cuando el servidor de acceso remoto detecta en alguno de sus módems (internos o externos) una señal de solicitud de acceso este lo valida y autentifica como un primer nivel de seguridad con un USER ID y un PASSWORD, una vez autentificado y validado este le asigna una dirección IP Dinámica o Estática (según se allá especificado en la configuración)

5. Una vez establecida la conexión el dispositivo tiene la posibilidad, si es que se le especifico dar servicio de DIAL BACK o DIAL OUT.

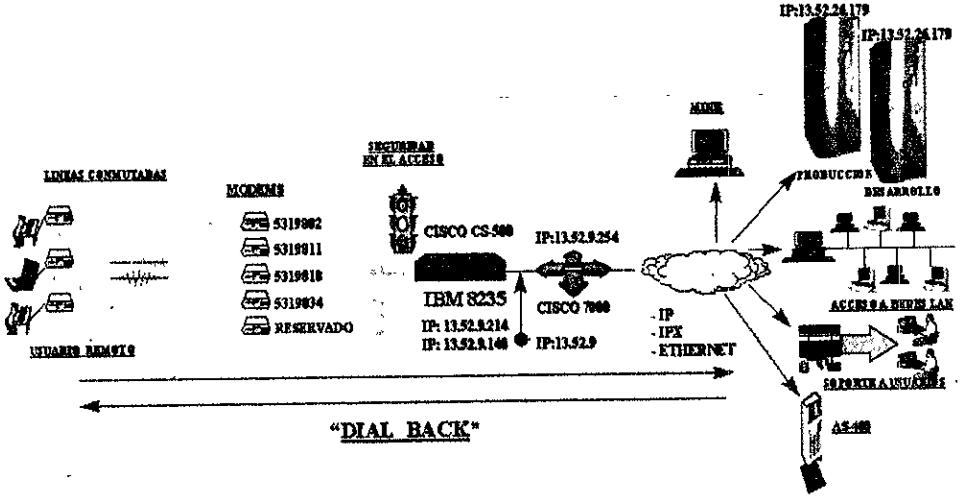
6. Una vez establecida la comunicación puede un usuario estar conectado a la red, y hacer accesos si tiene algún usuario y password a los servidores Novell, equipos bajo sistema

operativo Unix, equipos AS4000, RISC y minicomputadoras en general, así como el mismo Mainframe.

La seguridad es un punto muy importante, como primer nivel se pide un password y un user en el servidor de acceso remoto una vez pasado este nivel se verifica y valida en un servidor de accesos Kerberos, Network Bandery de Novell, o un servidor TACACS Pasado este nivel según sé allá especificado podrá tener acceso solo a ciertas rutas de acceso o segmentos. Otro nivel más es que debe tener acceso al o los diferentes sistemas para poder accesorios.

7. Un nivel más es el que permite generar una base de datos con información de los evento y accesos por parte de los usuarios que se están suscitando en el transcurso del día.

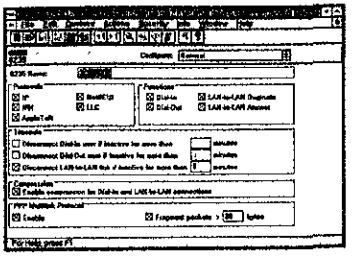
La gráfica muestra la forma en que se encuentra conectado un servidor de comunicaciones como el SHIVA, 8235-IBM o Bien un Cisco CS500 la ventaja del los dos primero en comparación con el CS-500 o el 2500 de Cisco es que tiene una innterface de configuración y administración más amigable.



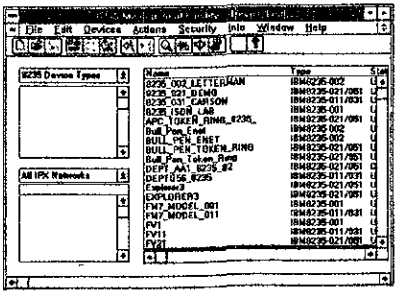
"Aplicación del IBM 8235"

Ventanas de configuración del Servidor de Comunicaciones

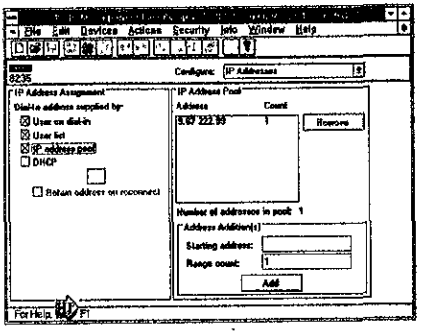
A continuación se muestran algunas de las ventanas de configuración y administración de este dispositivo:



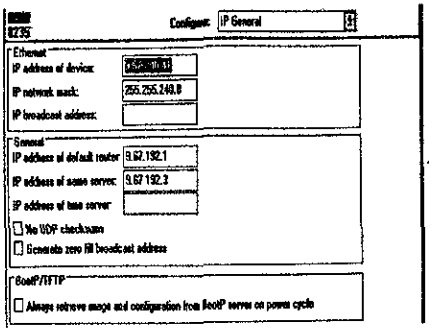
Ventana de configuración general



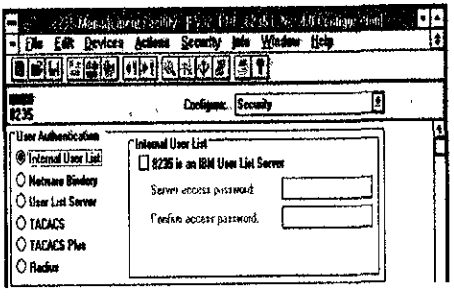
Ventana de selección de dispositivos



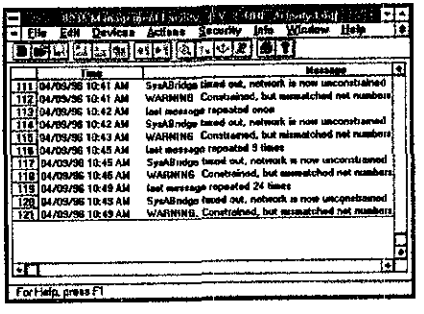
Ventana de configuración de pool de direcciones



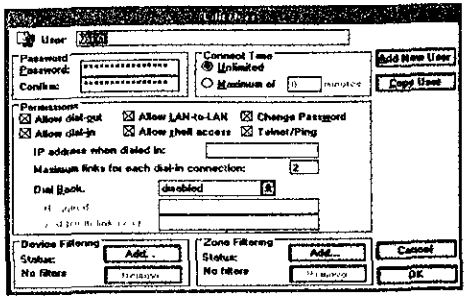
Ventana de configuración general de direcciones IP



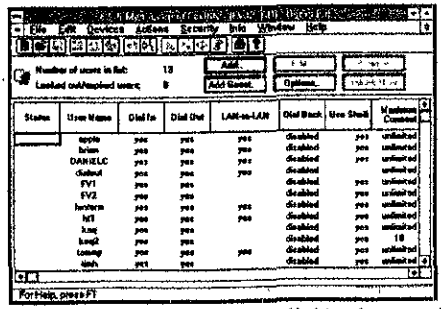
Ventana de configuración de niveles de seguridad



Ventana que muestra información de accesos al sistema



Ventana que muestra lista de usuarios



Ventana de configuración y edición de usuarios

V.2. ALTERNATIVAS DE SU USO.

Existen algunas decenas aplicaciones que se pueden implementar con este tipo de esquema de acceso moto como se muestra a continuación.

Soporte a usuarios remotos

Implementado el mismo esquema, le permite a usuarios remotos conectarse a la red corporativa vía una línea conmutada al servidor de comunicaciones tal como si estuvieran conectados físicamente, obviamente no con la misma velocidad de 10Mbs, pero si a 28800 o 33600 baudios. Al conectarse los usuarios remotos les permite tener control sobre sus archivos de red así como enviar y recibir correo, conectarse a otros equipos dentro de la red, etc.

Soporte Técnico Remoto

Permite a usuarios que dan soporte técnico(administradores, Supervisores o personal que tiene que ver de una u otra forma con el mantenimiento de la red) conectarse desde su casa, hotel si se encuentra de viaje en el interior de la república, para dar mantenimiento a los sistemas de la red corporativa, sin necesidad de presentarse a las instalaciones de la compañía. Ya que muchas veces solo hay que reinicializar los equipos, configurar ruteadores, correr procesos en el Mainframe, o bien dar mantenimiento al sistema operativo del Mainframe, o configurar equipo de comunicaciones, esto es una gran ventaja por que el tiempo de respuesta para la solución del problema se reduce, sin tener que perder tiempo en trasladarse de un lugar a otro donde se encuentra el problema.

Usuarios Externos

Al implementar este esquema se puede tener seguridad de acceso a usuarios externos (esto es otras compañías) que no se desea que anden navegando por nuestra red, con este esquema podemos delimitar con rutas estáticas de acceso, para que únicamente entren a determinados segmentos de red, así como mini-computadoras.

Cobranza Local y foránea Móvil

Actualmente se lanzo un proyecto piloto de cobranza de recibos telefónicos a colonias, esto funciona de la siguiente manera se implemento con el sistema de acceso remoto, esto es en lugar de un usuario remoto sea una computadora la cual esta siendo operada por una persona que realiza las funciones de cajera de banco y además esta se encuentra dentro de un camión blindado (de los que utilizan los bancos para transportar dinero) habilitando una ventanilla de cobro pasando por las colonias de la ciudad cobrando su recibo telefónico. Y la terminal o computadora conectada con telefonía celular y marcando al servidor de comunicaciones, y posteriormente al MainFrame donde se encuentra corriendo los programas necesarios para realizar los cobros. La señorita de la estación móvil consulta e imprime su talón de pago. Sin la necesidad de que el abonado tenga que ir a la sucursal.

Conexión LAN / LAN

Es un esquema que puede implementarse con el servicio de acceso remoto que permite conectar 2 o más redes LAN para formar una sola. De tal forma que usuarios de una red pueden ver y compartir recursos con los otros usuarios de la otra red, y viceversa. A través de líneas conmutadas o privadas. Ahorrando así costos.

Implementación del mismo concepto pero con un equipo Cisco CS-500, cisco 2509 o 2500

Nota: al inicio de esta tesis el sistema de acceso remoto se pensaba como una alternativa de nueva tecnología, pero como uno sabe dentro de este ambiente de las comunicaciones y la computación se avanza a pasos agigantados, es por ello que al concluir con la presente tesis ya se encuentra implementado en esta compañía.

V.3. RED APPN.

APPN (Advanced Peer-to-Peer Networking) Redes Avanzadas tipo Igual a Igual Extensines SNA que proporcionan dirección intermedia de nodos, servicio dinámico de redes y una administración mejorada. Utiliza protocolos LU 6.2 y realiza en Nodo SNA Tipo 2.1.

LU 6.2 También llamado APPC (Advanced Program-to-Program Comunications) Comunicaciones Avanzadas de Programa a Programa Sesión SNA que proporciona comunicaciones entre dos programas de aplicaciones. Cuando se utiliza en un nodo SNA Tipo 2.0 permite que PCs o computadoras de rango medio, ejecutando sus propios programas, se comuniquen con el computador central. Cuando se utiliza en un nodo SNA Tipo 2.1, mantiene comunicaciones par a par entre todas las otras computadoras de nodo Tipo 2.1 sin pasar por la central.

APPC

(Advanced-Program-to-Program-Communications) Comunicaciones Avanzadas de Programa a Programa Término comercial de IBM para comunicaciones entre programas que utilizan protocolos SNA LU 6.2

V.4. FAST ETHERNET.

ATM

Basados en la IEEE,CCITT y ANSI se puede decir que ATM es solo un protocolo de ensamblaje y de desenblaje de paquetes de longitud fija de 53 octetos (5 de encabezados y 48 de información) en donde su encabezado contiene información de ruteo, control de errores, etc. ; las celdas así formadas son totalmente transparentes al protocolo empleado en el nivel FISICO (que será el SDH en el caso del BISDN).

Otra consideración "la característica más atractiva de utilizar ATM es su capacidad de proporcionar un gran ancho de banda". abe mencionar que si ATM puede realizar esto es debido la utilización de SDH en los enlaces. Es posible desarrollar cualquier otro protocolo que utilice un gran ancho de banda, pero no lo es tanto elaborar uno que sea tan flexible y universal como ATM, que serían las características más atractivas, no por nada a quedado para su utilización en la futura red BISDN.

V.5. INTERNET.

Existen 3 formas de conexión a la super carretera de información INTERNET:

1. Conexión de su computadora a su propia red LAN y esta a un HOST de Internet
2. Conexión Vía telefónica con protocolo SLIP o PPP a un HOST de Internet
3. Conexión a través de un servicio de correo electrónico (BBS).

En los dos primeros casos la conexión es directa. Una vez que se corre el software de TCP/IP en una computadora, este la convierte en un nodo más de Internet. La tercera es una conexión indirecta, esto significa que requiere de un tercero para su conexión como lo son los correos electrónicos (BBS).La diferencia entre conexión directa e indirecta es que en el primer caso se requiere de un mayor conocimiento del internet, mientras que en el segundo caso Servicios en línea adicionan características de ayuda que permiten interactuar con Internet que los hacen más fácil de navegar por la super carretera de la información. Además de ofrecer el servicio de correo electrónico. Delphi, American On Line son algunos de los medios que ofrecen estos servicios.

	Conexión a Red	Conexión SLIP/PPP	Conexión de Servicios BBS
Requerimiento	Requiere de una computadora que este conectada a una red y que esta red este conectada a Internet, además de una tarjeta de red y el drive que controle la tarjeta ODI, NDIS. También necesita correr el software TCP/IP Si se esta corriendo bajo Windows se requerirá de Un Winsock.	Se requiere un modem de preferencia que soporte SNMP y por lo menos una velocidad de 14.4Kbps.	
Beneficios	Se puede accesar a toda la información y servicios que ofrece Internet como Mail, Noticias, Servidores de Ghopers, servidores de Web´s y mucho más		
Costo	El costo de la conexión como lineas de datos: E1, . T1, líneas dedicadas de 56kbps, switches de 56kbps. los cuales incrementan el costo. Además del software necesario como TCP/IP y winsock.		

CONCLUSIONES.

Ante la globalización de los mercados internacionales y la utilización de nuevas tecnologías y sin caer en un punto de vista simplista, pensamos que el próximo milenio estará regido por la Telemática, donde no podemos decir que las computadoras alcancen su máximo desarrollo, debido a que este es ilimitado, como ilimitada es la capacidad humana y seguramente las futuras generaciones serán testigos de avances sumamente espectaculares que en estos momentos no son aceptados por la gente, no por que no existan, sino por que en este momento no tenemos la tecnología para concebir nuevas formas de comunicación, esto nos conduce a la gran necesidad de capacitar a estas generaciones cada vez de una manera más completa e integral, con el propósito de generar en ellos una visión más completa de lo que representa la ingeniería en los mercados globalizados.

Por otra parte, también es importante inculcar una actitud cada vez más abierta a todo tipo de cambios y principalmente a los tecnológicos ya que en cuestión de días, cosas que son muy novedosas en este momento, se hacen obsoletas con el paso del tiempo.

Estamos convencidos que los ingenieros de sistemas deberán estar inmersos en los conceptos de la computación tratando de abarcar todas y cada una de sus áreas, con el propósito de tomar decisiones más rápidamente y además que estas sean las más adecuadas, también estamos conscientes que se puede pensar que esto representa una tarea titánica a desarrollar, sin embargo el entorno de las nuevas generaciones les hace más fácil alcanzar este objetivo.

La interconexión de redes en los últimos años ha tenido un gran auge, sobre todo con el surgimiento de Internet, el mantener el control de las transacciones y comunicación entre redes de una manera ágil es importante, esto se logra mediante un centro de control que pueda administrar y monitorear los recursos de la red o las redes.

BIBLIOGRAFÍA.

Building Industry Consulting Service International, Telecommunications Distribution Methods Manual, 5ta. Ed.
(Lexington, Ky: Publication Group, GTE TestMark Laboratories, 1994)

Patrick H. Corrigan y Aisling Guy, Building Local Area Networks with Novell's NetWare v.2.2 and 3.11, (Redwood
City, California: M&T Publishing, Inc., 1992)

Dyson, Peter, Novell's Dictionary of Networking, (San José, California: Novell Press, 1994)

Electronics Industry Association/Telecommunications Industry Association, EIA/TIA Building Telecommunications
Wiring Stantards, (Englewood, Colorado: Global Engineering Documents, 1992)

International Business Machines, IBM Token Ring Network Telephone Twisted-Pair Media Guide, 4ta. Ed. (Armonk,
N.Y.: IBM, 1986)

Mark Miller, LAN Troubleshooting Handbook (Redwood City, California: M&T Publishing, Inc., 1989)

Bryan Pfaffenger, Que's Computer User's Dictionary, 2a Ed. (Carmel, Indiana: Que Corporation, 1991)

Russel Sanders, "Mapping The Wiring Maze", LAN Technology, 15 Octubre 1992.

Comer, Duglas E. 1991 internetworking with TCP/IP, Pretice Hall Inc. Englewood Cliff. NJ.

Camppel Laura. 1993. Novell´s Guide To Netware LAN Analyzer. Sybex

Edmunds, Jonh J. 1992 SAA/LU 6.2 Distributed Network and Aplication, McGraw Hill. Inc. New York

Mos barger, Myron. 199. "Wide Area Networking Wint VSAM:

customer Instalation. " Network Aplication Notes"Dec. 1993: Novell Inc.

IBM Skill Dynamics Dallas Tx..IBM TCP/IP for MVS course Code CG37880C Student Guide

Sterling Software,1997, CONNECT Direct introduction for MVS. 2477 Gateway Drive-suit 101 IrvingTx.

IBM Managing your APPN Enviroments Using NETVIEW., April 1996, Raleigh Center GC24-2559-00

Tannenbaum, Todd. 1993. The Point To Point Protocol, WAN Connection, Nov. 1993CMP Publication INC

PAGINAS.

WWW.BYTE. COM
WWW.CISCO.COM
WWW.CMAGAZINE.COM
WWW.DISCOVERY.COM
WWW.EXCEED.COM
WWW.ICROSOFT.COM
WWW.IMB.COM
WWW.INTERNET.COM
WWW.NASA.COM
WWW.NET.COM
WWW.NEXTSTEP.COM
WWW.NOVELL.COM
WWW.SPECTRUM.COM
WWW.TP.COM
WWW.UN.COM
WWW.SERPIENTE.DGSCA.UNAM.MX
WWW.HP-720.ARAGON.UNAM.MX
WWW.INDY.ARAGON.UNAM.MX