Universidad Nacional Autónoma de México

Escuela Nacional de Estudios Profesionales

A R A G O N

"EL CONTROLADOR LATTISNET EN EL MONITOREO DE UNA RED LOCAL"

FALLA DE ORIGEN

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A :

EDUARDO MENA MARTINEZ

Asesor: ING. SILVIA VEGA MUYTOY

San Juan de Aragón, Edo. de México Noviembre de 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DEDICATORIAS:

A mi padre:

Te dedico este trabajo como muestra de mi cariño que te tengo, y te doy las gracias por el apoyo y confianza que has depositado en mí, te quiero mucho papá.

A mi madre ✝ :

Tu ausencia me hizo madurar tempranamente y aprender a valorar la vida y a la gente que aún tengo conmigo, así como también me motivo a mejorar como ser humano y ser más responsable y honesto. Donde quiera que te encuentres, te amo con toda el alma.

A mis hermanos :

Gabriel, Rocio y Alex, les dedico este trabajo con mucho cariño y quiero decirles que lo realice pensando en ustedes.

A mi gran familia:

Por creer en mi, gracias a todos Abuelos, tios, primos, sobrinos y amigos.

AGRADECIMIENTOS:

Ing. Silvia Vega Muytoy:

Por la confianza y apoyo incondicional recibido desinteresadamente y por creer en mí.

A la UNAM:

Por haberme dado la oportunidad de realizar mi licenciatura en este plantel y demostrar lo que ahora soy.

Al Centro de Cómputo de la ENEP Aragón:

Por darme la oportunidad de haberme iniciado profesionalmente en este centro, agradezco el apoyo que me dieron cada uno de los elementos que ahí laboran.

" EL CONTROLADOR LATTISNET EN EL MONITOREO DE UNA RED LOCAL "

INTRODUCCION

La palabra comunicación proviene del verbo latino communicare, derivado de communis "común", por lo tanto, la comunicación que denota la acción y el efecto de comunicar , encierra en esencia la noción de hacer común algo. La facultad de transmitir lo que sabe distingue al ser humano del resto de la creación, puesto que, desde tiempo atrás, ha manifestado a sus congéneres sus ideas, descubrimientos e invenciones.

El hombre ha desarrollado las comunicaciones hasta superar con amplitud la fase de la señal física o corporal, buena prueba de ello son el lenguaje, la imprenta, el servicio de correos, los libros, los periódicos y revistas, el teléfono, el telégrafo, la radio, la televisión, el cine, los discos, las computadoras, etc.

Pero para el tema en esencia, la era de la comunicación electrónica se inicia en 1834 con la invención del telégrafo el cual se lo debemos a Samuel Morse, no obstante la importancia de este invento tenía como defecto la automatización de la transmisión, debido a la incapacidad de sincronizar unidades de envío y recepción automática.

Fue hasta el año de 1874 cuando Emil Baudot ideo el código en el cual el número de elementos en una señal era el mismo para cada carácter y la duración (sincronización) de cada elemento era constante, ese código fue llamado de longitud constante. Los trabajos de sincronización comenzaron con el desarrollo de la máquina de escribir de teclado telcimpresora en 1869.

Fue hasta 1910 cuando el americano Howard Krun introdujo mejoras en el concepto de la sincronización y lo aplicó al uso de equipos automáticos de telegrafía.

En 1928 las teleimpresoras habían sido mecanizadas y se incorporaban un lector y un perforador de cinta de papel accionado por teclado, transmitían ya fuera directamente por medio del teclado o por medio de la cinta y el producto final era cinta perforada o bien una copia impresa.

El primer equipo teleimpresor operaba sin ningún protocolo ; se alineaba el mensaje de cinta o se metía el mensaje por medio de teclado, tan pronto como la máquina local comenzaba a transmitir, la máquina receptora copiaba la transmisión.

A medida que las comunicaciones se volvieron más sofisticadas, en el comienzo de los años 50 se introdujeron dispositivos electromecánicos centrales para realizar tareas como invitación notificando en secuencia a cada estación del mismo circuito para transmitir su tráfico, y selección notificando a una determinada estación que debe recibir un mensaje. Para adaptarse al control adicional requerido para estas funciones, se equipó a las teleimpresoras con dispositivos que decodificaban secuencias de caracteres. Esto permitió a la teleimpresora enviar, recibir, reacondicionar o realizar alguna otra función básica.

Dado que la mayoría de estas teleimpresoras operaban con el código de Baudot , que no permite realizar funciones de control excepto la alimentación de línea y el retorno de carro, se usaba una serie de diferentes caracteres alfabéticos llamados secuencias de control para comandos de control específicos. Este fue realmente el origen de los protocolos de comunicación de datos.

Anteriormente con la invención del telégrafo también se dio la invención del teléfono, con esto, se permitía la comunicación por medio de la voz y el telégrafo a través de la misma línea, valiéndose de la comunicación alternada.

En 1920 ya se habían establecido los principios básicos de telecomunicaciones , conmutación de mensajes y control de línea. Los sistemas se construyeron con base en comunicaciones a través de la voz y transmisión de caracteres de datos.

Más tarde surge el desarrollo comercial del computador, pero como estas primeras máquinas estaban orientadas a lotes, no existía la más mínima necesidad de interconectarse con algún sistema de comunicación, sin embargo, la industria tomó conciencia de la conveniencia de que máquinas y gente hablarán entre si, dado que el único sistema de comunicación disponible era el telefónico, los computadores en evolución habrían de desarrollarse siguiendo vías que les permitieran usar este servicio.

En tanto el crecimiento del uso de la comunicación fue simultáneo al crecimiento de la tecnología de los computadores y en parte favorecido por él, las redes de conmutación de mensajes, reservación y transacciones financieras de los años 50's y 60's usaban computadores centralizados comparativamente sofisticados para controlar grandes poblaciones de dispositivos y terminales primitivas, pero a medida que estas redes crecían en lo referente a volúmenes de tráfico y crecimiento de terminales, el aspecto no controlado de la operación de las mismas terminales se volvió inaceptable.

En los años 60's las aplicaciones de comunicación de datos se expandieron más allá del intercambio de tráfico de mensajes, con la tecnología disponible se lograron velocidades más altas, más terminales en un circuito dado, mejor control de errores y otras mejoras. Estos adelantos tecnológicos y los cambios en la aplicación requirieron modificaciones en los protocolos que se usaban, como resultado los procedimientos de datos asíncronos reemplazaron a los protocolos de teleimpresoras mecánicas.

Pero afines de los 60's las operaciones sincrónicas reemplazaron los métodos asincrónicos. Las técnicas de transmisión sincrónicas fue en gran parte el resultado de presiones provenientes de la creciente popularidad de las

comunicaciones como algo anexo a la computación de uso general. Para explotar las mayores velocidades disponibles y para implantar los grados de control más sofisticados requeridos, los vendedores desarrollaron nuevos protocolos , el más conocido fue el desarrollado por la IBM y llamado "Comunicaciones Sincrónicas Binarias (BSC)", sin embargo se tuvo que este variaba de una clase de dispositivo a otro y de un fabricante a otro. El resultado final fue un número de versiones BSC en la actualidad incompatibles.

Al mismo tiempo que BSC alcanzaba sus límites, surgía otra orientación: "Procesamiento Distribuido de Datos". En un sistema de bases de datos distribuido, los datos se almacenan en varias computadoras las cuales se comunican entre si a través de diversos medios de comunicación, como pueden ser cables paralelos de alta velocidad o líneas telefónicas, estas no comparten la memoria principal.

Los procesadores de un sistema distribuido pueden variar en cuanto a su tamaño y función, pueden incluir microcomputadoras pequeñas, estaciones de trabajo, minicomputadoras y sistemas de cómputo grandes de aplicación general. Estos procesadores reciben diferentes nombres como son: localidades, nodos, computadoras, para este trabajo se denominarán nodos.

El sistema distribuido de datos consiste en un conjunto de nodos, cada uno de los cuales puede participar en la ejecución de transacciones que accesen datos de uno o varios nodos. La diferencia principal entre los sistemas de datos centralizados y distribuidos es que en los primeros, los datos residen en un solo nodo, mientras que los segundos se encuentran en varios nodos.

Los nodos del sistema pueden conectarse físicamente de diversas formas, punto que se tratará en capitulo posterior, pero que de antemano se menciona que las diferentes configuraciones de conexión deben contemplar lo siguiente:

* Costo de instalación.- es el costo de conectar físicamente los nodos del sistema

* Costo de comunicaciones.- es el costo en tiempo y dinero que implica enviar una transacción de un nodo a otro.

* Confiabilidad.- es la frecuencia con que falla una línea de comunicación o un nodo.

* Disponibilidad.- es la posibilidad de accesar la información a pesar de fallas en algunos nodos o líneas de comunicación.

Como se verá, estas características juegan un papel importante en la elección del mecanismo apropiado para manejar la distribución de los datos o información.

Los nodos de un sistemas pueden estar dispersos de manera física ya sea un área geográfica extensa (todo un país) o en un área reducida (un edificio o varios adyacentes). Una red del primer tipo se denomina red de larga distancia (WAN), mientras que el segundo se conoce como red de área local (LAN).

Puesto que los nodos de las redes de larga distancia están distribuidas en forma física en área geográfica extensa, es probable que las líneas de comunicación sean relativamente lentas y menos confiables en comparación con las redes de área local. Las líneas de comunicación de larga distancia normales son las líneas telefónicas, conexiones de microondas y canales de satélite, por otra parte, como todos los nodos de las redes de área local están próximos entre sí, las líneas de comunicación son de más alta velocidad y menor tasa de errores que sus contrapartes en las redes de larga distancias. Las conexiones más comunes son cables par trenzados, coaxiales de banda base, coaxiales de banda ancha y fibras ópticas.

El monitoreo a través de algún software y equipo en especial depende del tipo de configuración de la red que se este trabajando y del costo del mismo. Es muy importante llevar un control del monitoreo independientemente del tipo de configuración de la red, ya que nos da un status del funcionamiento de la red e incluso de realizar un mantenimiento preventivo o correctivo en alguno de los dispositivos que componen la red y así evitar el mal funcionamiento del envío de la información de un nodo a otro de una área especifica o un área tipo WAN.

1.1. OBJETIVOS

Objetivo Principal:

Describir las caracteristicas y funciones principales del controlador Lattisnet asi como sus componentes principales, para utilizar a este como una herramienta en el monitoreo de una red local y obtener el máximo aprovechamiento de la misma red.

Objetivos Particulares:

Describir cada uno de los diferentes protocolos más comunes que existen.

Describir las caracteristicas de una red local.

Identificar los componentes del controlador lattisnet y sus funciones .

Describir los canales Ethernet del controlador.

Identificar las funciones que realiza el NMM (Netware Management Module; Módulo administrador de RED)

Describir la forma de trabajar de los puentes en el controlador lattisnet.

Describir la forma de segmentar una red usando el módulo 3328 Ethernet Switching Engine (Mecanismo de conmutación Ethernet)

Explicar la forma de reconfigurar una red para facilitar el más rápido acceso a los servidores de la red.

Identificar los componentes y caracteristicas del programa Optivity para HP OpenView/DOS para el monitoreo de la LAN

Identificar el hardware, software y todos los requerimientos para la instalación del programa Optivity en el monitoreo de la LAN.

Describir la forma de configurar los modulos de administración de red (NMM's) a través de BootP/TFTP.

El presente documento esta compuesto de tal forma que sea entendible lo que es una LAN así como el producto Lattisnet Synoptics 3000 como hardware de monitoreo en la misma LAN.

En el capítulo "Protocolos de Comunicación" se tendra un panorama general en lo que consiste el modelo OSI ("Open System Interconect" ; Interconexión abierta de sistemas), las partes o módulos que conforman un cableado estructurado en el edificio de alguna empresa, así como los diferentes protocolos que existen en día en el mercado,

En el capítulo "Configuración de una red Local", se verá las características generales de una red de área local como son: topologías, componentes, protocolos, medios de transmisión.

En el capítulo "El manejador lattisnet", se describirá en que consiste dicho controlador, sus características principales y los módulos que lo componen.

En el capítulo "Procedimiento para el monitoreo de una red local" , se describió la forma de administrar un ambiente de red, por medio del software Optivity que va ligado de la mano con el manejador Lattisnet.

Por último se tendrá las conclusiones al respecto del trabajo de tesis.

2. PROTOCOLOS DE COMUNICACIÓN

2.1 MODELO OSI

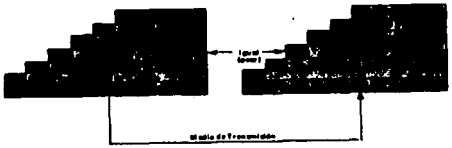
2.1.1. Introducción

Debido a que la industria de computo creció como respuesta a las exigencias del mercado, los fabricantes crearon equipos y dispositivos para satisfacer la demanda del momento. Sin embargo, todos esos equipos que en ese momento cubrieron la demanda no son compatibles entre si. Los fabricantes los construyeron con tecnología propietaria y sin ningún estándar o regla. Esto no fue problema hasta que surgieron las redes o la necesidad de interconectar sistemas disímiles. La interoperabilidad entre dispositivos de diferentes fabricantes se vuelve extremadamente difícil. Es como tratar de que un chino y un ruso se entiendan sin establecer regla alguna o un idioma común.

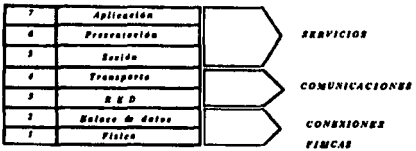
En 1977, la ISO ("International Organization for Standarization" ; Organización Internacional para la estandarización), organismo formado por representantes de la industria, creó un comité para desarrollar estándares para la comunicación de datos, y con esto lograr la interoperabilidad entre sistemas heterogéneos. El resultado de este esfuerzo fue un modelo de referencia conocido como el modelo de referencia OSI ("Open Systems Interconnect" ; Interconexión de sistemas abiertos) o el modelo de referencia para la Interconexión de Sistemas Abiertos.

El modelo OSI sirve como guía o una serie de lineamientos para las tareas de comunicación, no especifica un estándar de comunicación, sin embargo, muchos estándares y protocolos cumplen con lo que establece el modelo.

Siempre se ha dicho que para resolver un problema es mejor dividirlo en partes más pequeñas y resolver cada una de las partes. Esto es precisamente lo que hace el modelo OSI; divide el problema de la comunicación en siete partes o capas, cada una de las capas destinada a una tarea especifica.



Cada capa ofrece o solicita servicios de las capas adyacentes. Cada capa se comunica con su igual en el dispositivo receptor, es decir, la capa 4 del nodo A solo se puede comunicar con la capa 4 del dispositivo B. Cada capa agrega el mensaje original cierta información de control conocida como Encabezado. En el equipo receptor, cada capa va quitando el encabezado para que el usuario reciba el mensaje original.



Como se muestra en la figura, las capas del modelo OSI se pueden agrupar en categorías de acuerdo a su funcionalidad:

Conexiones Físicas (capas 1 y 2): estas capas proveen la conexión física a la red y son responsables de mover la información sobre el medio de transmisión.

Comunicaciones (capas 3 y 4): estas capas son responsables de que la información sea transportada de manera confiable desde el dispositivo transmisor hasta el receptor, independientemente del medio físico.

Servicios (capas 5,6 y 7): estas capas tienen como responsabilidad ofrecer servicios de red al usuario, por ejemplo, servicios de impresión, emulación de terminal, validación de acceso, traducciones de formato, entre otros.

Dependiendo de la capa de OSI de la que estemos hablando es como referimos a la unidad de información, aunque esta nomenclatura no es un estándar:

7. Aplicación	**Mensaje**	**Conversación**
6. Presentación	**Mensaje**	**Diálogo**
5. Sesión	**Mensaje**	**Párrafo**
4. Transporte	**Datagrama**	**Oración**
3. Red	**Paquete**	**Frase**
2. Enlace de datos	**Marco de información**	**Palabras**
1. Física	**Bits**	**Letras**

El modelo OSI no es tangible, sólo especifica que tareas deben llevarse a cabo en cada capa, más no dice como se deben realizar. El modelo OSI hay que verlo como un marco de referencia en base al cual se desarrollan los protocolos que posteriormente implementan los fabricantes.

2.1.2 Capas físicas

* *Capa física, capa 1* .- La capa física se ocupa de la tranamisión de bits a lo largo de un canal de comunicación. Esta capa describe las especificaciones físicas del medio, como son: el tipo de cable, las propiedades eléctricas y funcionales de las señales de transmisión y recepción, entre otros. Esta capa es la responsable de transmitir y recibir bits a través del medio de tranamisión.

* *Capa de enlace de datos, capa 2*.- La capa de enlace de datos es responsable de organizar los bits que llegan de la capa 1 en marcos de información. Un marco de información es una agrupación de bits con significado.

Esta capa agrega cierta información de control al mensaje original, tal como la dirección física (MAC Adress o dirección de hardware) del emisor y del destinatario, longitud del marco de información y un indicador del protocolo superior involucrado. Controla además el acceso al medio.

Esta capa se subdivide en dos subcapas:

a) *LLC ("Logical Link Control" ; Control de enlace lógico)* .- que ofrece dos tipos de servicios: Servicios orientados a conexión (Connection Oriented) y servicios no orientados a conexión (Connectionless).

b) *MAC ("Media Access Control"; Control de acceso al medio).*- que controla el acceso al medio, maneja las direcciones físicas o de MAC, forma los marcos de información.

* *Capa de RED, Capa 3*.- El objetivo principal de la capa de red es el de mover información a través de varias redes interconectadas entre si, o sea una interred. Esta capa se encarga de colocar el paquete en la red destino, basándose en direcciones lógicas o direcciones de red.

A esta capa también se le conoce como capa de ruteo, pues sus funciones principales son la de ruteo y conmutación de la información. Es en esta capa donde residen los protocolos como IP ("internet address" ; dirección Internet) e IPX ("Internetworking Packet eXchange"; Intercambio de paquetes de interconexión de redes), quienes se encargan de encontrar el camino óptimo para que el mensaje viaje de la red origen a la red destino.

* *Capa de transporte, Capa 4*.- La capa de transporte funciona a la mitad del modelo OSI. Esta capa asegura una entrega confiable de información entre el emisor y el receptor. La palabra "confiable" no quiere decir que la información siempre va a ser entregada, si se rompe el cable de la red, la información nunca llegará a su destino. Sin embargo, la capa 4 sabe que la información no llegó y lo avisa a las capas superiores para que retransmitan el mensaje e implementan un mecanismo comparable con el correo certificado.

Para ser confiable esta capa implementa varios mecanismos como el manejo de confirmaciones o acuse de recibo por cada datagrama que se envía lleva secuencia de cada datagrama, establece circuitos virtuales, etc. Ejemplo de protocolos de capa 4 son: TCP ("Transmission Control Protocol"; Protocolo de control de transmisiones), SPX ("Sequenced Packet eXchange" ; Intercambio de paquetes secuenciales).

• *Capa de sesión, Capa 5*.- La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. Una sesión podría permitir al usuario acceder a un sistema de computo distante o transferir un archivo entre dos nodos.

Uno de los servicios de la capa de sesión consiste en administrar y controlar el diálogo. Las sesiones permiten que el trafico vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si el trafico solo puede ir en una dirección en un momento dado, la capa de sesión ayudará en el seguimiento de quien tiene el turno. La capa de sesión negocia el establecimiento de conexiones, autentifica el acceso al servidor, coordina y sincroniza el diálogo y provee la administración de la sesión.

• *Capa de presentación, capa 6* .- La capa de presentación realiza las funciones de traductor. A diferencia de las capas inferiores que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

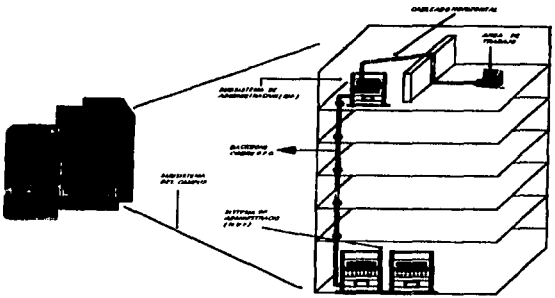
Un ejemplo típico de las funciones de esta capa es la traducción entre formatos de archivos ASCII ("American Standard Code for Information Interchange"; Código Estándar Norteamericano para intercambio de información)-EBCDIC ("Extended Binary Code Decimal Interchange Code" ; Código de intercambio decimal codificado en binario). El trabajo de manejar estas estructuras de datos abstractos y la conversión de la representación utilizada en el interior de la computadora a la representación normal de red, se lleva a cabo a través

de la capa de presentación. Otros ejemplos de funciones de la capa de presentación son la compresión de datos y el encriptamiento.

• *Capa de aplicación, capa 7.*- En esta capa no residen las aplicaciones con las que trabaja el usuario. Aquí residen los protocolos necesarios para ofrecer los servicios de red. Un ejemplo es el correo electrónico. En la capa 7 reside un protocolo para correo electrónico con la función de que un mensaje de correo llegue del emisor al destinatario, pero esto no es lo que ve el usuario. El usuario utiliza una interfase para crear el mensaje y para enviarlo. Distintas interfases de usuario (de varios fabricantes) pueden utilizar el mismo protocolo de mensajería.

2.2 CABLEADO ESTRUCTURADO

La metodología para el diseño de un sistema de cableado para la comunicación de datos consiste en dividir el sistema dentro de un marco de módulos. Esto permite la modificación de los módulos con un mínimo impacto sobre los demás. En otras palabras modularidad significa cambios sencillos y oportunidad de crecimiento.



Así contamos con los siguientes módulos:

* *Sistema de administración MDF ("Main Distribution Frame"; Distribución principal de servidores)*: área donde se localizan los equipos (servidores, concentradores, patch panels, etc.) que permiten el enlace entre los usuarios de la red. Normalmente se le conoce como el área del SITE, pero en muchas ocasiones no es necesario tener un MDF, pues se puede optar por tener varios IDF. Es desde este elemento donde parte o se inicia el cable estructurado, pues da cabida a los demás subsistemas.

* *Sub-sistema medular/dorsal o backbone (conocido también como el subsistema vertical)*: es el medio por donde corre la información hacia los demás niveles en un edificio, proviene desde el sistema de administración para concluir en los IDF's. El elemento de comunicación puede ser de fibra óptica (Backbone colapsado), coaxial grueso (RG11), coaxial delgado (RG58) o de cable UTP ("Unshielded twisted Pair"; Par Trenzado sin protección). La elección del tipo de backbone esta totalmente ligada a las necesidades o parámetros a cubrir por la red, como lo son: el número de usuarios, ambiente en la red, paqueterías, distancias entre los módulos de administración y necesidades de los equipos.

* *Sub-sistema de administración IDF ("Intermedial Distribution Frame"; Distribución intermedia de servidores)*: este módulo recibe la información del backbone y la distribuye entre los usuarios de la red en su área, también aquí es posible tener administración directa sobre los equipos que lo componen, como son los patch panel's, concentradores, receptores de fibra óptica (LIU). Es por ello que se puede tener tantos IDF's como sean necesarios. Es este módulo el que da el comienzo al Subsistema de Cableado Horizontal.

* *Sub-sistema horizontal*: proviene del módulo IDF, parte desde los patch panels hacia el área de trabajo. El medio de comunicación o enlace más común entre estos dos subsistemas, es el cable telefónico UTP, de categoría 5. La distribución del cable se realiza principalmente por encima de los plafones falsos (con tubería) o bien por el área perimetral (por canaletas) con la finalidad de no afectar la estética de los inmuebles o por facilidad y bajo costo, según sea el caso.

* *Sub-sistema del área de trabajo*: este módulo es el punto final del cableado estructurado, pues es aquí en donde se termina o "remata" el cable proveniente del IDF en los jacks RJ45 o rosetas. Posteriormente con un cable

UTP que contenga conectores RJ45 en sus extremos, conocidos como cables de extensión o patch cordon, se da entrada a la PC en la red. En la mayoría de los casos el cable UTP se conectorizan los 8 hilos con la finalidad de estar preparado para cambios futuros de un tipo de red Token Ring a Ethernet o viceversa.

• *Sub-sistema de campo*: se entiende como el medio por el que se realiza la conexión entre los sistemas de administración de diferentes edificios cercanos. Los medios más usados para la interconexión son la fibra óptica para exteriores y el cable coaxial grueso (RG11), siendo el primero el de mayor demanda principalmente por el manejo de grandes distancias, así como la velocidad de la misma.

Estos sub-sistemas o módulos mantienen un alto grado de independencia. Por lo tanto los cambios en un sub-sistema no afectan a los otros sub-sistemas. La modularidad del cableado estructurado permite a la red crecer en forma continua y ordenada según las necesidades lo requieran. Lo anterior se encuentra basado principalmente en la planeación del cableado estructurado, pues se procura dejar los materiales de enlace un 50 % de posibilidad de crecimiento.

Finalmente, una vez que se tiene la infraestructura establecida, los costos en tiempo y dinero se reducen significativamente en la ampliación del cableado.

Entre la ventaja principal que nos proporciona el sistema de cableado estructurado esta principalmente el Costo: todo cambio, mantenimiento y movimiento se realiza sin problema.

La interoperabilidad debe tener las siguientes características:

1) *Universal*: combina y se adapta al equipo de voz y datos de diferentes distribuidores a su sencillo estándar de cableado.

2) *Expansión*: el cable UTP asegura la no obsolescencia del cableado, protagonista importante en el mundo de la transferencia de datos de alta velocidad, además de ser multiprotocolo.

3) *Garantía*: es un sistema garantizado contra cualquier falla.

4) *Compatible*: cualquier equipo (sin importar el fabricante) que se comunique con cable UTP puede adaptar su interfase para convivir en una red de cableado aprobado.

El tiempo ocioso de una red puede ser extremadamente caro para cualquier organización. Cada componente dentro del sistema de información debe ser confiable. Se ha encontrado que los problemas relacionados con el sistema de cableado representan un 70% de los que se generan en la red.

Este aspecto le agrega otra dimensión a la selección de un sistema de cableado: considerar la confiabilidad de un sistema antes de implantarlo. Esta confiabilidad influye el comportamiento eléctrico, la integridad de la terminación del cable y la inmunidad a la interferencia.

Al considerar que el cableado es una inversión en equipo y programas para transmisión de datos, una elección sabia radica en hacer la inversión hoy para no tener que hacer una más fuerte mañana.

El sistema de cableado es un componente estratégico dentro del plan general de los sistemas de información. Por esta razón debería planearse e implantarse tomando en cuenta firmemente los beneficios a largo plazo, las consideraciones de costo y el rendimiento general.

2.3 PROTOCOLOS

2.3.1 Definición

A menudo existe confusión en la industria de las comunicaciones de redes sobre las diferencias entre el modelo OSI, protocolos de red y la implementación de un protocolo. Al empezar a trabajar en la selección y diseño de dispositivos , servicios y productos de administración de LAN/WAN resulta de mucha ayuda el entender como difieren los conceptos antes mencionados.

Un modelo representa conceptos generales y guías de como se debe mover la información de un lugar a otro. Describe ciertos servicios que deben ser proporcionados y que capa es responsable de hacerlo.

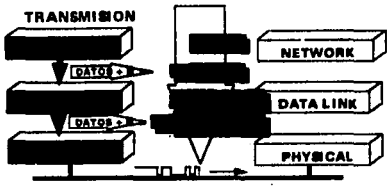
Un protocolo es un conjunto de reglas concernientes al hardware, procedimientos y estructuras de datos. Es el "plano" que siguen los desarrolladores para crear productos de hardware y software que de echo muevan información a través de una red o que provean servicios de red. Típicamente un protocolo trata con solo una capa del modelo.

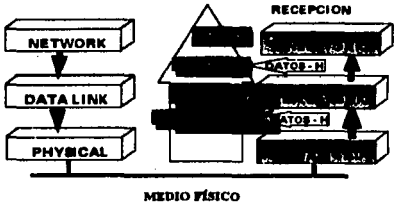
Una implementación es la forma en que un fabricante crea un producto basado en un protocolo. Por último, cabe mencionar que una arquitectura específica en forma exacta, los servicios y protocolos que se utilizaran en cada una de las capas de un modelo.

En una red de área local (LAN) todos los nodos conectados requieren de un protocolo de comunicaciones que pueda transportar información de un nodo a otro. Estos protocolos operan en diferentes capas del modelo OSI.

Así encontramos que en las primeras dos capas del modelo se definen los protocolos que se encargan de accesar el medio físico de comunicaciones; así como de generar los marcos de información correspondientes a una determinada tecnología de LAN, como Ethernet, Token Ring (red basada en conectar nodos en forma circular a través de un anillo) o FDDI ("Fiber Distribuited Data Interfase" ; Interfaz de datos distribuidos por fibra) entre otras.

Cada marco de información lleva datos provenientes de las capas superiores en las que intervienen protocolos, cuya función es la de "mover" datos de un nodo a otro una vez que se encapsuló la información en un servidor. También se encarga de entregarla o recibirla desencapsulada del frame al medio, según sea el caso de transmitir o recibir respectivamente.





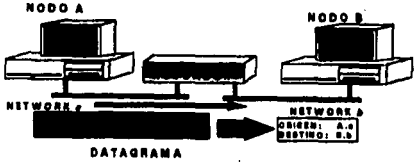
Podemos encontrar una gran variedad de los protocolos que están funcionando sobre la capa 2 del modelo OSI, ya que las diferentes arquitecturas de cómputo y teleinformática hacen uso de propietarios de la arquitectura , protocolos estándares o tal vez una combinación de ellos.

Existen diferencias fundamentales entre protocolos superiores a capa 2 del modelo OSI, aunque todos ellos tienen la misma función. Una de sus principales características es la de permitir catalogarlos como protocolos ruteables y no ruteables; además de que cada uno de estos protocolos, sea ruteable o no, puede ser o no orientado a la conexión.

2.3.2 Protocolos ruteables

Un protocolo ruteable puede definirse como aquel que "interpreta" al origen y al destino de la información que llevan consigo sus paquetes, como un ente lógico denominado red. En efecto, cada segmento físico de LAN es definido como una dirección lógica.

En la siguiente figura se puede observar que el nodo A de la red A envía datos al nodo B que se encuentra en la red B. El protocolo es capaz de interpretar la dirección lógica de la red A como el origen en donde se genera la información del nodo A, y la dirección lógica B como el destino.



Cuando el protocolo percibe esto, prepara dentro del paquete de información un formato con el remitente y destinatario de esta unidad de información. A continuación el software de red, corriendo en el nodo A, en este caso encapsula este paquete en un marco de información Ethernet y lo transmite por medio de comunicación. El ruteador conectado a ese segmento de red recibe el marco de información y lo "lee". Si el ruteador posee la habilidad de interpretar cual es el protocolo ruteable que genero el paquete encapsulado en el servidor, esto es, si cuenta con el software que habilita el proceso de ruteo para este protocolo, entonces el ruteador lo retransmitirá por la interfase que lo conecta por la red b. Esto lo consigue porque el ruteador también es capaz de comprender el origen y el destino de esta información. A este proceso se le conoce como ruteo de información

Los protocolos ruteables guardan una analogía con el servicio de correo. Los paquetes destinados a un nodo llevan dentro de si un formato conocido como encabezado (header) que lleva la información de la dirección de red origen (calle del remitente) y de la red destino (calle del destinatario), y puede llevar también el número de nodo origen (No. de casa del remitente) y el número del nodo destino (No. de casa del destinatario). En la analogía el número de red es el nombre de la calle y el número de nodo (MAC Address o nodo físico), es el número de la calle que estamos buscando.

Todos los protocolos ruteables se caracterizan por definir un origen y un destino a la información que propagan. Cuando se diseña y configura una red que opera con protocolos ruteables cada segmento físico de red debe definirse como una red lógica. Esto se aplica tanto a segmentos LAN como a segmentos WAN.

Volviendo a la analogía del servicio de correo, hay protocolos ruteables que se asemejan a un servicio de correo certificado. En este el cartero nos devuelve un acuse de recibo firmado por el destinatario en el momento de la recepción. De esta forma se garantiza que el mensaje (carta) ha sido llevado hasta su destino sin contratiempos. De igual forma, algunos protocolos ruteables solicitan un reconocimiento por parte del destinatario de que este ha recibido el paquete de información.

Puesto que este proceso se realiza miles de veces durante una sesión normal de trabajo, el efecto final es como si ambos nodos mantuvieran una conversación constante entre ellos, y tal pareciera que los computadores se encontraran conectados entre si mediante una "conexión virtual". De ahí el nombre de que el protocolo se "orienta" a mantener esa conexión virtual. A estos protocolos se les conoce como protocolos orientados a la conexión (connection oriented protocols).

Los protocolos ruteables que no se orientan a una conexión, son como el correo ordinario. Si usted envía una carta y nunca le contestan, no tiene manera de saber si esta fue entregada al destinatario o si simplemente se

extravío. De igual manera los protocolos no orientados a la conexión no garantiza que la información transmitida se envíe íntegramente.

La mayoría de los protocolos ruteables que operan en la capa 3 del modelo OSI no son orientados a la conexión. Para ofrecer un servicio orientado a la conexión requieren de un protocolo de capa superior. Tal es el caso por ejemplo de IPX, que no esta orientado a la conexión, pero que lo consigue transfiriendo su información al protocolo de capa superior inmediata que si esta orientado a la conexión, en este caso el protocolo SPX. Lo mismo podemos decir del protocolo IP con su protocolo superior TCP.

La ventaja de los protocolos no orientados a la conexión sobre los otros es que por lo general son más rápidos; ya que no tienen que ejecutar algoritmos de verificación de transmisión y tampoco tiene que esperar los reconocimientos de los paquetes transmitidos. Sin embargo, estos protocolos no detectan ni corrigen errores, ni se recuperan de fallas en la transmisión. En la mayoría de los casos le dejan estas tareas a protocolos de capas superiores.

A continuación se presentan características de algunos de los protocolos ruteables más importantes:

Nombre: IPX/SPX ("Internetwork Packet eXchanged/Sequenced Packet eXchange"; Intercambio de paquetes de interconexión de redes/ intercambio de paquetes secuenciales)

Tipo: Estándar de la industria

Desarrollado por: Novell Inc.

Usado por: Netware, servidores de aplicación y diversos clientes.

Direcciones de: 8 bytes para red, 12 bytes par a nodo

Características: Es el protocolo que usa la arquitectura de Novell. Introducido al mercado en 1983 opera virtualmente sobre cualquier plataforma de hardware. IPX no es orientado a la conexión, SPX si lo es. Otros

protocolos auxiliares son RIP ("Routing Information Protocol"; Protocolo de información de enrutamiento) para el intercambio de información de ruteo, SAP ("Service Advertising Protocol" ; Punto de acceso al servicio) para notificar la presencia de los servidores y sus servicios; y NCP ("Netware Core Protocol"; Programa de control de la red) que regula las sesiones de trabajo entre el servidor y el cliente. Existen varios clientes que se comunican con el file server usando IPX entre los que se pueden citar Macintosh, UNIX, OS/2, Dos, Windows NT, Windows for Workgroups, etc. IPX es adecuado para redes de área local, pero no se recomienda para enlaces de red de área amplia de velocidades inferiores a 65 Kbits/s, aunque existen técnicas para mejorar su rendimiento.

Nombre: TCP/IP ("Transmition Control Protocol/Internet Protocol" ; Protocolo de control de transmisiones/Protocolo Internet)

Tipo: Estándar de la industria

Desarrollado por: DoD USA

Usado por: Unix, Netware, SNA, Windows NT, OS/2 y muchos clientes mas.

Direcciones de: 4 bytes (para red y nodo)

Características: El Transmition Control Protocol/Internet Protocol, busca facilitar la comunicación entre computadores de múltiples arquitecturas. Se le encuentra prácticamente en todas, las arquitecturas de cómputo actuales, IP no es orientado a la conexión, TCP si lo es. Desarrollado desde los principios de los 70's, hoy en día es uno de los protocolos más utilizados a nivel mundial. TCP/IP se utiliza para definir a una familia de protocolos que proveen múltiples servicios de interconexión de redes entre los que destacan: ARP ("Address Resolution Protocol" ; Protocolo de resolución de direcciones) para mapear direcciones lógicas en físicas; RIP ("Routing Information Protocol" ; Protocolo de información de enrutamiento), para intercambio de información de ruteo; ICMP ("Internet Cotrol Message Protocol" ; Protocolo Internet de control de mensajes), que reporta condiciones de error en la red; UDP ("User Datagram Protocol" ; Protocolo de datagrama de usuario), protocolo de transporte similar a TCP pero no es orientado a la conexión; FTP ("File Transfer Protocol" ; Protocolo de transferencia de archivos), usado para transferencia de archivos; TELNET que provee servicios de emulación de terminal; NFS ("Network File

System" ; Sistema de archivos en red) que provee acceso transparente a diferentes sistemas de archivo; RCP ("Remote Procedure Calls" ; Procedimiento de llamadas remota), sirve para disparar procesos remotos, SNMP ("Simple Network Management Protocol" ; Protocolo Simple de Manejo de Redes), usado para el control, monitoreo y administración de los dispositivos que componen la red. La familia de protocolos de TCP/IP provee mecanismos de detección de fallas y en ocasiones puede recuperarse de ellas. Esto lo sitúa como uno de los protocolos más usados para conexión tanto LAN como WAN. Una de las grandes ventajas de este protocolo es que puede operarse sobre muy diversas plataformas de hardware de comunicaciones, esto ha provocado que pueda encontrarse en una heterogénea mezcla de arquitecturas tanto de cómputo como de comunicaciones.

Nombre: Apple Talk

Tipo: estándar propietario

Desarrollado por: Apple Computer Inc.

Usado por: Macintosh, Netware, Windows NT, etc.

Direcciones de: 2 bytes para red, 1 byte para nodo

Características: Apple Talk no sólo es una familia de protocolos, sino también una arquitectura. Originalmente diseñada para servir a las redes de computadora Macintosh, pero se ha convertido en uno de los protocolos más socorridos. Para cuestiones de interoperabilidad, muchas otras arquitecturas se comunican con Apple Talk para integrarse al mundo de las Macintosh. Todos los protocolos de esta familia están diseñadas para facilitar las tareas que el usuario tiene que hacer para crear una red de computo debido a la filosofía de la compañía. Apple Talk requiere para su operación crear no solo redes lógicas por segmento físico, también grupos lógicos de redes llamados "zonas". Entre los principales protocolos que conforman la familia se tienen: DDP (Deliver Datagram Protocol), no esta orientado a la conexión y es el responsable de mover los datos entre redes; NBP (Name Binding Protocol), que se encarga de convertir los servicios de red en un nombre comprensible para el usuario y las aplicaciones; ZIP (Zone Information Proocol) sus mensajes propagan la presencia de las "zonas" lógicas de la red; ATP (Apple Transaction Protocol), similar a DDP pero si es orientado a la conexión; RTMP (Routing Table

maintenance Protocol), su propósito es mantener actualizadas las tablas de ruteo en los ruteadores que operan con los protocolos de Apple Talk.

Debido a que se trata de una arquitectura propietaria que cubre las siete capas del modelo OSI, Apple Talk cuenta con muchos otros protocolos que le dan la característica principal y que consiste en simplificar las tareas que debe hacer el usuario para accesar no solo al computador sino a la red y todos sus servicios.

Nombre: DecNet (Digital equipment Corporation Network)

Tipo: Estandar propietario

Desarrollado por: Digital Equipment Corp.

Usado por: Equipos DEC, Gateways y clientes

Direcciones de: 2 bytes (6 bits para red, 6 para red en fase IV), 48 bits (en fase V)

Características: Siendo una arquitectura propietaria, cuenta con una serie de protocolos que cubre todos los servicios de red. Sin embargo, DecNet se caracteriza por ser una arquitectura abierta, lo que le da versatilidad para integrarse con otras plataformas tanto con protocolos propietarios como estándares, sobre todo en DecNet fase V, donde DEC optó por los protocolos propuestos en el modelo OSI.

Dada la enorme cantidad de estos equipos en el mundo sobre todo la fase IV, se considera que sus protocolos son ruteables. Las redes en DecNet fase IV se denominan "áreas" y estas pueden extenderse por varios segmentos físicos. Pero un ruteador que "entiende" DecNet puede mover la información de un área a otra en un verdadero proceso de ruteo.

En DecNet fase V, DEC mantiene un firme compromiso de mantener su arquitectura abierta y compatible con el modelo OSI. Esto lo demuestra al integrar como parte de su serie de protocolos, los especificados en cada capa del modelo OSI.

Los protocolos que llevan información en DecNet fase IV no son orientados a la conexión, pero se utilizan varios protocolos de control para mantener las sesiones de trabajo. Entre ellos tenemos a: DRP(DecNet Routing Protocol) que se encarga de las funciones de ruteo y transporte de información; y NSP (Network Services •Protocol) que equivale a un protocolo de la capa de transporte que esta orientado a la conexión.

Nombre: OSI

Tipo: Estándar Internacional

Desarrollado por: International Organization for Standarization

Usado por: DEC fase V y otras arquitecturas abiertas

Direcciones de: 48 bits

Características: El modelo OSI también define sus propios protocolos para las capas de red y de transporte. A nivel de red OSI propone dos protocolos: CLNS (Connection Less Network Service) y CONS (Connection Oriented Network Service). Como sus nombres lo indican, el primero es un protocolo de red No orientado a la conexión y el segundo si lo es. OSI también propone un protocolo de red derivado de X.25. Este se conoce como X.25 Nivel 3.

Para la capa de Transporte OSI utiliza una serie de protocolos que proveen diferentes tipos de servicios. Esos protocolos se identifican como TP0, TP1, TP2 y hasta TP4, TP es por Transport Protocol y mientras que TP0 es un protocolo muy sencillo con servicios simples, los demás van aumentando su grado de complejidad y los servicios que ofrecen hasta llegar a TP4.

A pesar de que el modelo OSI define toda una familia de protocolos y servicios muy completos, muy pocas arquitecturas de cómputo los han adoptado.

Nombre: X.25

Tipo: Estándar Internacional

Desarrollado por: Comite Consultivo Internacional de Telefonía y telegrafía

Usado por: Prácticamente todas las arquitecturas de computo y comunicaciones.

Direcciones de: 15 bytes

Características: Se desarrollo en la segunda mitad de los 70's y fue ideado para crear redes de comunicaciones para múltiples plataformas de cómputo que operan sobre una red publica de paquetes conmutados. TelePAC y TeleNET son ejemplos de ese tipo de redes. Hoy en día los costos de instalación de este tipo de redes han bajado considerablemente, de tal forma que se pueden crear redes de paquetes conmutados de carácter privado. Esencialmente X.25 es un protocolo para crear redes WAN. Cada enlace WAN es un segmento de red de una inter-red X.25. Se pueden instalar sobre cualquier medio físico de comunicaciones remotas como líneas telefónicas, enlaces satelitales, microondas, enlaces digitales de RDI, etc. Su instalación se recomienda para enlaces de baja velocidad hasta de no más de 256 Kilobits/s. X.25 es un protocolo orientado a la conexión y utiliza el concepto de circuitos virtuales para crear esa conexión lógica. Muchos protocolos modernos que caen dentro de la denominación de "paquetes conmutados" deben su desarrollo a las experiencias con el protocolo de X.25.

Nombre: Frame Relay

Tipo: Estándar Internacional

Desarrollado por: Varios fabricantes, el American Standar Institute y la CCITT

Usado por: Mayor parte de arquitecturas de comunicaciones

Direcciones de: 10 bits (actual), 17 bits (futuro), 24 bits (futuro).

Características: Muchas de las características de X.25 se pueden encontrar en F. Relay. También es un protocolo orientado a la conexión y opera bajo el concepto de conmutación de paquetes. Puede instalarse en redes publicas o privadas y al igual que X.25 el tamaño de sus paquetes es variable. Frame Relay puede funcionar sobre cualquier plataforma de comunicaciones remota. Es adecuado principalmente para operar a velocidades superiores a 64

Kbits/s; y una de las ventajas que tiene sobre X.25 es su relativa simplicidad de operación y control, lo que mejora el uso del ancho de banda. Se debe recordar que X.25 es un protocolo desarrollado hace casi 20 años y fue diseñado para proteger la información que viajaría por líneas telefónicas poco confiables, tarea que consumen muchos recursos en los equipos de comunicaciones. Frame Relay aprovecha la confiabilidad de los enlaces digitales modernos y sus recursos se enfocan al manejo eficiente de la información que transporta.

Nombre: ATM ("Asynchronous Transfer Mode"; Modo de transferencia asicrónica)

Tipo: Estándar Internacional

Desarrollado por: ATM for UM

Usado por: Principales fabricantes de equipo de interconexión de redes

Direcciones de: 2 bytes

Características: ATM es un protocolo ruteable orientado a la conexión, que utiliza técnicas de conmutación de celdas de información. La conmutación de paquetes permite que el tamaño de las unidades de información sea variable, en conmutación de celdas, este valor es fijo. ATM opera a altas velocidades de transmisión llegando incluso hasta los 622.08 Mbits/s y como sus unidades de información son fijas, puede transportar lo mismo voz, datos e imágenes en tiempo real. Otra característica fundamental de ATM, es que es un protocolo que define desde las primeras capas del modelo OSI y permite extender sus servicios desde redes LAN a toda clase de redes con enlaces WAN. Esta versatilidad pronostica una amplia aceptación para el diseño e implantación de futuras interredes.

Nombre: PPP ("Point to Point" ; Punto a Punto)

Tipo: Estándar de la industria

Desarrollado por: Internet Activities Board

Usado por: Equipos de comunicaciones que "entienden" TCP/IP

Direcciones de: 8 bits en capa 2, 4 bytes en capa 3

Características: El Point to Point Protocol es un protocolo asincrono de comunicaciones para enlaces WAN tipo punto a punto. Forma parte del set de protocolos de TCP/IP, pero es considerado como un protocolo para WAN porque permite encapsular información que no necesariamente debe ser TCP/IP. Este protocolo entiende el concepto de "red" en el sentido de que conoce de que red viene y a que red va, pero no es un protocolo que permita integrar redes LAN con WAN en forma transparente, debido a que PPP es un vínculo entre redes, y cada segmento configurado con PPP es una red por si sola.

2.3.3. Protocolos no ruteables

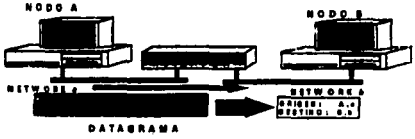
Como su nombre lo indica, estos protocolos no son susceptibles de ser ruteados. Si no existe ruteo, no existe el concepto de red lógica. Para este tipo de protocolos el entorno de comunicaciones se desenvuelve en una sola red. Estos protocolos están diseñados para reconocer como único mecanismo de control de comunicaciones entre los nodos a las direcciones físicas de los nodos. Esa dirección física es conocida como el número de nodo o la dirección de MAC (Media Access Control).

Retomando la analogía con el servicio de correo, un protocolo no ruteable sería como un servicio de correo en donde el único dato para reconocer el remitente y destinatario serían los números de casa de una sola calle. Es decir, en este servicio de correo sólo existe una calle a la cual dirigir la correspondencia. De la misma manera los protocolos no ruteables asumen que están comunicando nodos de una sola red de área local.

Al conectar varios segmentos físicos de red entre sí, es decir, al crear una interred, ya sea con segmentos de LAN o segmentos de WAN, debemos utilizar un dispositivo de interconexión de redes conocido como puente. Un puente es un elemento de comunicaciones que sólo propaga las direcciones físicas de los nodos. Por esta razón, los puentes permiten extender los segmentos físicos de red y hacen parecer a los protocolos no ruteables, como una sola red a todos los segmentos interconectados con puentes. Hay que recordar que no existe el concepto de red

lógica desde el punto de vista de los protocolos no ruteables, por lo tanto a estos protocolos sólo les interesa saber direcciones físicas de cada nodo

Para este propósito los puentes crean en sus memorias una tabla de direcciones físicas para saber si propagan los marcos de información (frames) generados en un segmento de red hacia otros segmentos.



Los protocolos no ruteables generalmente no son "comprendidos" por los puentes, por lo tanto la información de control contenida en los paquetes de información no es interpretada por los puentes. La dirección de MAC es suficiente para que los protocolos no ruteables hagan su trabajo de mover información de un nodo a otro. Esto nos lleva a pensar que los protocolos no ruteables propagan la información más rápido que los protocolos ruteables, y de hecho un puente es un dispositivo de interconexión de redes más rápido que un ruteador. Pero para interredes muy grandes la eficiencia decae con el uso de este tipo de protocolos. Por otro lado, muchos protocolos no ruteables no están diseñados para operar en ambientes WAN, porque al asumir que se encuentran en un ambiente de una sola red, demandan todo el ancho de banda disponible, que es un lujo que difícilmente nos podemos dar cuando estamos interconectando nuestras redes con enlaces WAN.

Al igual que los protocolos ruteables, los no ruteables se dividen en orientados a la conexión y no orientados. Además los protocolos no ruteables generalmente abarcan los servicios de comunicación de nodos de LAN, desde la capa 2 del modelo OSI hasta las últimas capas de éste.

A continuación se encuentran algunos de los protocolos no ruteables más comunes y sus principales características:

Nombre: APPC ("Advanced Peer-toPeer networking" ; Comunicación avanzada entre nodos similares), NetBios ("Networking basiv Input/Ouput System" ; Sistema Básico de entrada/salida de red), NetBEUI ("NetBIOS Extended User Interfase"; Interfase de usuario extendido NetBIOS).

Tipo: Estándar propietario

Desarrollado por: International Business Machines Corp.

Usado por: Equipos IBM, Gateways y clientes

Direcciones de: 12 bytes

Características: El 60% de las redes de cómputo hoy en día utilizan algún equipo de arquitectura propietario de IBM SNA ("Standar Network Architecture" ; Arquitectura de redes de sistemas). IBM originalmente desarrolló esta arquitectura basada en grandes procesadores centrales que atendían un gran número de terminales tontas. Pero al integrarse en las nuevas tecnologías de LAN, IBM tuvo que idear nuevos protocolos más eficientes. NetBIOS (Network Basic Input Output System), que consiste en un protocolo de alto rendimiento a nivel LAN y que utiliza la dirección física de cada nodo para mover la información; NetBUI (NetBIOS Extended User Interfase), es similar a NetBIOS pero permite encapsular la información en un formato LLC2 que es de reciente creación. APPC (Advanced Program to Program Communication) es otro protocolo propietario de IBM más versátil y complejo que anteriores, pero diseñado para operar con las nuevas interfases físicas que vienen en los equipos de comunicaciones de la arquitectura SNA de IBM. Todos estos protocolos no ruteables, operan eficientemente en ambientes LAN, pero en WAN consume muchos recursos y ancho de banda, por lo que no se recomienda extender su uso a largo de una WAN.

Nombre: SNA ("Systems Network Architecture" ; Arquitectura de redes de sistemas)

Tipo: Estándar propietario

Desarrollado por: International Business Machines Corp.

Direcciones de: 2 bytes (WAN), 12 bytes (LAN)

Características: Presentada en 1974, la arquitectura SNA es una de las más utilizadas debido a la gran aceptación de los equipos IBM que utilizan esta arquitectura. Durante más de una década SNA se mantuvo como una plataforma monolítica y cerrada, de tal forma que para poder interconectar equipos entre si debían ser de la misma naturaleza, ya que SNA utilizó protocolos y esquemas de comunicación propietarios. Con el éxito que tuvieron las LAN's en la década de los 80's, IBM rompió con su viejo esquema de computo centralizado para incursionar en el distribuido. Para lograr esto, SNA fue modificado para aceptar información transportada por protocolos de LAN. Los desarrollos que IBM realizó sobre Token Ring dieron como resultado que aunque el estándar internacional de Token Ring (802.5) se acepta como lo conocemos actualmente, en realidad se trata de una implantación y modificación del Token Ring original, hecho por IBM.

SNA operado sobre Token Ring puede utilizar algún protocolo de LAN que no es ruteable. Los protocolos usados son LLC2 donde un puerto lógico (Service Access Point), es usado para entregar y recibir información que solo los equipos IBM entienden; el otro protocolo usado por IBM es NetBIOS.

Recientemente IBM ha conseguido implantar protocolos ruteables a sus equipos de SNA. Ahora ya se pueden encontrar conexiones tanto en Token Ring como Ethernet (FDDI inclusive), que pueden comunicarse con TCP/IP.

Al adoptar IBM este tipo de tecnologías, se consigue una mejor interconexión de equipos de arquitectura SNA con plataformas de otras arquitecturas diferentes.

Es importante para una buena conectividad el saber si el equipo SNA que pretende ser integrado con otras arquitecturas, esta utilizando protocolos no ruteables como LLC2 o NetBIOS, o un protocolo ruteable como TCPIP.

Nombre: LLC2 (Logical Link Control 2)

Tipo: Estándar internacional

Desarrollado por: Proyecto 802 de la IEEE

Usado por: Equipos IBM, gateways y clientes, Windows NT, Novell, OS/2, etc.

Direcciones de: 12 bytes (MAC)

Características: El proyecto 802 de la IEEE define dos tipos de encapsulamiento de un marco de información para diferentes tipos de LAN: 802.3 para Ethernet y 802.5 para Token Ring. Pero define sobre estos un formato más, el 802.2 que le da ciertas ventajas de comunicación cuando se pasa la información de cada marco de información a las capas superiores. En esas capas pueden estar operando muchos y diferentes protocolos de muy diversas arquitecturas. Un método eficiente de entregar esa información es utilizar un puerto lógico (SAP) a cada uno de esos protocolos, así se consigue que un sólo formato de frame pueda intercambiarse fácilmente información de una plataforma a otra. LLc2 asigna un número de identificación a cada fabricante y/o protocolo de capa superior. Como LLC2 opera en la capa 2 del modelo OSI, se comporta como un protocolo no ruteable, ya que lo único que maneja para llevar información de un nodo a otro es la dirección física.

Nombre: DEC LAT , DEC LAN Bridge

Tipo: Estándar propietario

Desarrollado por: Digital Equipment Corp.

Usado por: Equipos DEC, Terminal Servers.

Direcciones de: 12 bytes (MAC)

Características: En ciertos equipos de DEC se utiliza el protocolo de LAT (Local Area Transport) principalmente para conectar terminales tontas de minicomputadores DEC, usando una red Ethernet como medio de comunicación. Este protocolo asume que el servidor que atiende a las terminales y siempre esta conectado al mismo segmento de LAN. Esto lo constituye como un protocolo no ruteable. DEC LAN Bridge es un protocolo de DEC que permite extender las redes de VAX, que son computadores de tecnología DEX a través de varios segmentos de LAN. Este

protocolo consigue su propósito haciendo el trabajo de un protocolo de Puente. Esto implica el uso de un dispositivo tipo puente que haga esa función.

Así concluimos este capítulo en cuanto a lo referente a protocolos, en este capítulo se describio cada una de las funciones de las capas de l modelo OSI, así como la descripción de los protocolos más cómunes en el mercado y en los cuales se describio a cada uno de estos.

3. CONFIGURACION DE UNA RED LOCAL

3.1 INTRODUCCION

El surgimiento de las microcomputadoras a fines de los 70's atrajo la atención de millones de usuarios que vieron en ellas la oportunidad de obtener capacidad de cómputo a bajo costo, con autonomía y versatilidad.

El mejoramiento de sus características, velocidad y capacidad del microprocesador, memoria principal y secundaria, les permitieron, no sólo capturar el mercado de estudiantes y usuarios particulares, sino también competir favorablemente contra minicomputadoras y equipos grandes en aplicaciones de negocios, en empresas de todos tamaños, al grado de desplazarlos paulatinamente de las salas de cómputo. Se estima que el mercado de las microcomputadoras tipo PC, crece anualmente al más del 50%, mientras que el de los equipos mayores crece en tasas menores al 15%.

Sin embargo, para alcanzar la amplia aceptación que han tenido las microcomputadoras, se han debido superar deficiencias que habían persistido pese al mejoramiento de sus capacidades individuales, por ejemplo, es altamente incostable conectar de manera dedicada cierto tipo de periféricos a cada microcomputadora de que se dispone. Igualmente ineficiente y costoso para una organización resulta el instalar software en cada microcomputadora, ya que ello implica duplicarlos n cantidad de veces.

La solución de esto y otros inconvenientes fue la estructuración de redes de microcomputadoras, es decir, la interconexión y operación de este tipo de equipos en un ambiente homogéneo, que les permitiera compartir recursos e información de manera eficiente. Las redes además han traído consigo ventajas adicionales respecto a los otros sistemas computacionales.

El concepto de red se ha ampliado enormemente, incluyendo equipos, minicomputadores y equipos grandes, rebasando el ámbito de una sala de cómputo hasta alcanzar con sus nodos, diversos puntos de una ciudad o de un país, utilizando como medio de conexión desde líneas telefónicas convencionales hasta las comunicaciones vía satélite.

Actualmente la tecnología de redes ha creado sus propias herramientas de programación y comunicaciones y se ha convertido en la rama de la computación con mayor desarrollo.

El mundo LAN nació por la necesidad de compartir recursos entre las computadoras y sus usuarios para hacer más eficientes, económico y administrable un sistema de computo.

Inicialmente se interconectaron 3,4 o 5 máquinas utilizando un sólo canal de transmisión y recepción para todas las terminales, las aplicaciones utilizadas eran DOS, no gráficas y generalmente los archivos transmitidos eran texto en código ASCII. Las redes funcionaban bien.

El problema comenzó con el cableado. Con la utilización del cable coaxial Ethernet o un anillo TOKEN Ring, añadir y mover usuarios se convirtió en una actividad de empalmes y conexiones defectuosas que ocasionaban problemás constantemente. Para solucionar este problema se inventaron los concentradores que ofrecen al exterior una topología en forma de estrella manteniendo ya sea el bus Ethernet o el anillo Token Ring en su interior. Esto solucionó los problemás ya que mover o añadir usuarios constituía un sólo cable y no todo un bus o un anillo.

Las aplicaciones se volvieron más complejas. Se integraron más usuarios y en consecuencia se demandaron más recursos de la red. El exceso de tráfico en un bus o en un anillo hicieron a las redes lentas e ineficientes. La solución surgió con la invención de los puentes que permitieron dividir la red en segmentos al interconectarlos en la red con la subsecuente división de tráfico.

Así surgió la necesidad de interconectar redes con diferentes topologías e identificarlas lógicamente para hacerlas administrables. Para resolver estos problemás de conectividad surgieron los ruteadores, que permitieron dividir tráfico, organizar segmentos lógicamente e interconectar redes de diferentes topologías.

Actualmente, por la complejidad de las aplicaciones y los volúmenes de información que se transfiere de un punto a otro, han surgido tecnologías que ofrecen anchos de bandas mayores y dedicados a cada usuarios denominados "conexiones orientadas", como ATM; así como dispositivos que procesan el tráfico a mayor velocidad y eficiencia al internarse en el mundo de la conmutación.

3.2 DEFINICION

Una red es un conjunto de dispositivos interconectados en un ambiente computacional para compartir información y recursos informáticos.

Los dispositivos pueden incluir computadoras de diversas configuraciones, terminales y periféricos tales como impresoras, lectoras de cinta magnética, digitalizadores, graficadores, entre otras cosas. Como parte de la red también se cuenta los medios de transmisión de datos como cables, satélites, módem, programás de comunicaciones.

En cuanto a las funciones, además de las que pueden desarrollar sus componentes por separado, las redes permiten la transferencia de archivos, el envio y recepción de mensajes (correo electrónico), la operación de aplicaciones desde varias estaciones de trabajo simultáneamente.

Los elementos con que cuenta una red pueden variar dependiendo de las funciones especificas para las que estén diseñada. Sin embargo, existen elementos comunes a todas ellas que son los que veremos a continuación:

Estación de trabajo o nodo.- son las computadoras o terminales desde las cuales el usuario puede utilizar la red.

Servidor.- es un dispositivo qué proporciona una función especial a todos los usuarios de la red. Entre los tipos de servidores más importantes se encuentran los siguientes:

- Servidor de archivos.- provee área de almacenamiento y acceso a programás y archivos de datos compartidos.
- Servidor de impresión.- controla las colas de impresión y da acceso a las impresoras conectadas a él.
- Servidor de bases de datos.- equipo dedicado al almacenamiento y organización de bases de datos y recuperación de los datos solicitados en las consultas.

En realidad los equipos que operan como servidores son computadoras semejantes a las que se utilizan como estaciones de trabajo o nodos, aunque generalmente con mayor capacidad, en los cuales se ejecuta un programa que les permite desempeñar la función especial que desarrollan. Cuando el equipo únicamente desempeña esa función se le llama servidor dedicado. Cuando además se utiliza como estación de trabajo se le llama servidor no dedicado.

Existen microcomputadoras muy poderosas (basadas en microprocesadores INTEL 80386, 80486 y actualmente pentium) que pueden desempeñar eficientemente varias funciones de servidores a la vez. A dichos equipos se les ha denominado servidores de redes.

Tarjeta de red.- tanto las estaciones de trabajo como los servidores se encuentran conectados entre sí mediante cables especiales. Cada equipo cuenta con una tarjeta o adaptador de red, a la que se conectan dichos cables y está diseñada para controlar las comunicaciones de la estación de trabajo con los demás puntos de la red.

Protocólo.- es el conjunto de reglas que se siguen para empacar la información que va a ser enviada por las estaciones de trabajo y los servidores de la red. Se considera como un lenguaje de la red. El protocolo es en realidad un elemento de la programación de las redes, pero se incluye en esta parte para asociarlo con los componentes físicos de las comunicaciones.

Sistema de cableado.- dentro de éste, se incluyen los cables y elementos adicionales asociados a ellos como caja de conexiones y conectores especiales, que se utilizan en la interconexión de los puntos de la red. Los tipos de cable más utilizados son básicamente tres y se enlistan a continuación:

* Par trenzado (Twisted-pair).- cable utilizado comúnmente en las instalaciones telefónicas domésticas, que se forma de dos alambres aislados que se tuercen entre sí. Pese a su popularidad, introduce distorsión y ruido en la línea cuando aumenta la distancia o la velocidad de transferencia, debido a sus características eléctricas. Esta deficiencia se han corregido en parte, agregándole un blindaje, aunque lo ha hecho más costoso

* Cable coaxial.- alambre sólido protegido por un aislante y una malla de metal cuyo eje de curvatura coincide con el del alambre, de donde se deriva su nombre. De mayor calidad que el par trenzado, pero más caro.

* Fibra óptica.- cable hecho de fibra de vidrio o plástico, a través del cual se emite un haz luminoso que se va reflejando dentro del cable debido a los diferentes índices de refracción entre éste y su cubierta. Su instalación es considerablemente más costosa que en los casos anteriores, ya que se requiere de cuidados y mantenimiento especial, aunque en condiciones adecuadas permite velocidades de transmisión más elevadas y mayores distancias. Se espera que con los avances técnicos se convierta en el cable del futuro.

3.3 CARACTERISTICAS

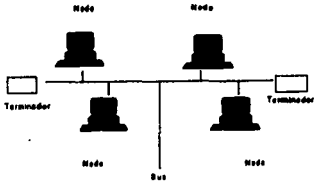
Una red local se caracteriza por tres aspectos: el medio de transmisión, topología y el método de acceso.

3.3. 1 Topologías

Siguiendo el modelo OSI nos situamos ahora en el nivel de enlace de datos. En este nivel se encuentran las topologías de red y los protocolos de acceso al medio. Actualmente en el universo de las redes hay numerosas topologías, entre las que destacan algunas que se han caracterizado por su rápida implementación, velocidad, flexibilidad y su tolerancia a fallas.

a) Bus lineal (Ethernet 10MB)

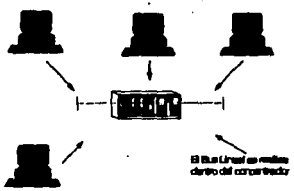
Consiste de una línea troncal (o bus) a la que están conectados todos los nodos. La señal viaja en ambas direcciones del cableado y es terminada en los extremos por medio de una resistencia (terminador) . Es posible cablearla a través de coaxial, par torcido o fibra óptica (utilizando concentradores en las dos últimas opciones). La velocidad de comunicación es de aproximadamente 10 MBps.



b) Bus lineal Modificado (Ethernet 10MB, Fast-Ethernet 100MB)

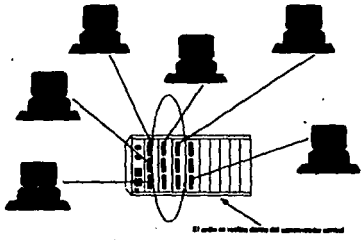
El bus lineal se encuentra de manera lógica dentro de un concentrador, al cual se conectan uno a uno los nodos formando una estrella. Típicamente este arreglo utiliza cable torcido (UTP o STP) , siendo utilizado en redes Ethernet a 10 o Fast-Ethernet a 100 MB, dependiendo de la tecnología que maneje el dispositivo.

La ventaja principal de esta topología es que si un nodo falla o se desconecta, el concentrador de inmediato restablece el bus lineal, evitando así la caída de la red. Como consecuencia de lo anterior descubrimos que es de fácil reubicación.



c) Anillo modificado (Token Ring)

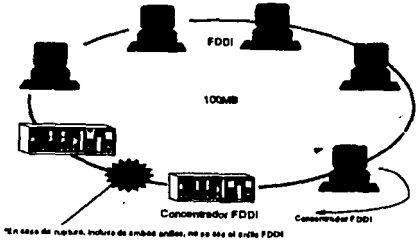
También conocida como estrella-anillo. El anillo se encuentra dentro de un ruteador de señal que puede ser un MAU ("Multistation Acces Unit" ; Unidad de acceso a multiestación), que hoy en *dia* se esta substituyendo por concentradores inteligentes, al cual se conectan uno a uno los nodos formando una estrella. La señal siempre pasa por el ruteador. Tipicamente este arreglo utiliza cable de par torcido (UTP o STP) a 4 0 16 Mbps. La ventaja de utilizar esta topología y no el anillo físico es que si un nodo falla o se desconecta, el concentrador de inmediato cierra el anillo evitando la caída de la red.



d) Anillo doble redundante (FDDI)

La topología de anillo doble redundante fue diseñada para redes FDDI (" Fiber Distributed Data Interfase" ; Interfaz de datos distribuidos por fibra) en donde se requiere alta velocidad. Las redes FDDI consiste en dos anillos de transmisión en contrasentido. El anillo primario es utilizado como canal principal. Si por alguna razón este anillo es interrumpido, el secundario restablece la continuidad del primario en forma automática, actuando como redundancia o anillo de respaldo.

Se utiliza como medio principal el cableado de fibra óptica y muy recientemente el cable UTP categoría 5 y cable STP. Con esta topología se puede alcanzar velocidades de 100 Mbps compartidas entre cada uno de los dispositivos conectados al doble anillo redundante.



3.3.2 Medios de transmisión

El medio de transmisión es la facilidad física usada para interconectar juntas estaciones de trabajo o nodos y dispositivos para crear una red que transporte mensajes entre las mismás.

La selección del medio de transmisión a utilizar depende de: tipo de ambiente donde se va instalar, tipo de equipo a usar, tipo de aplicación y requerimientos, capacidad económica (relación costo/beneficio).

Los medios físicos se dividen en:

1) Enlaces físicos terrestres: par de cables tocidos, cable coaxial de banda angosta y banda ancha, fibras ópticas.

2) Espacio aéreo: microondas, infrarrojo, laser y radio frecuencia.

Las características básicas de un medio de transmisión son:

1) Resistencia.- es la oposición al flujo de la corriente eléctrica, depende de longitud, diámetro y material usado en la construcción del circuito.

2) Inductancia.- es aquella propiedad de los conductores que tienen a oponerse a cualquier cambio en el campo magnético existente alrededor del alambre, y que depende de variables tales como: tamaño de alambre, forma, valor del flujo instantáneo de corriente y proximidad a otros conductores.

3) Capacitancia.- depende del tamaño absoluto de los conductores; del tamaño relativo respecto al otro; del espacio entre los mismos y del tipo de material dieléctrico que los separa.

Existen dos medios para llevar información de un punto a otro: compartido y conmutado. El medio independientemente de ser compartido o conmutado es el canal a través del cual se establece una comunicación.

El medio compartido fue el primero en utilizarse y se caracteriza por dar servicio a más de un usuario. Ejemplo de esto son Ethernet, Token Ring, FDDI, entre otros. En el caso de Ethernet, un sólo bus lleva la información de una estación al resto sin importar si va dirigida a una sola o a todas ellas, de tal forma que todas las estaciones "pelean" por la utilización del bus, en este caso el medio. En Token Ring, todas las estaciones comparte un anillo y el Token o estafeta pasa por todos los nodos sin importar si el paquete va dirigido o no a ellas. Caso similar ocurre con el FDDI.

Los medios físicos se dividen en:

1) Enlaces físicos terrestres: par de cables tocidos, cable coaxial de banda angosta y banda ancha, fibras ópticas.

2) Espacio aéreo: microondas, infrarrojo, laser y radio frecuencia.

Las características básicas de un medio de transmisión son:

1) Resistencia.- es la oposición al flujo de la corriente eléctrica, depende de longitud, diámetro y material usado en la construcción del circuito.

2) Inductancia.- es aquella propiedad de los conductores que tienen a oponerse a cualquier cambio en el campo magnético existente alrededor del alambre, y que depende de variables tales como: tamaño de alambre, forma, valor del flujo instantáneo de corriente y proximidad a otros conductores.

3) Capacitancia.- depende del tamaño absoluto de los conductores; del tamaño relativo respecto al otro; del espacio entre los mismos y del tipo de material dieléctrico que los separa.

Existen dos medios para llevar información de un punto a otro: compartido y conmutado. El medio independientemente de ser compartido o conmutado es el canal a través del cual se establece una comunicación.

El medio compartido fue el primero en utilizarse y se caracteriza por dar servicio a más de un usuario. Ejemplo de esto son Ethernet, Token Ring, FDDI, entre otros. En el caso de Ethernet, un sólo bus lleva la información de una estación al resto sin importar si va dirigida a una sola o a todas ellas, de tal forma que todas las estaciones "pelean" por la utilización del bus, en este caso el medio. En Token Ring, todas las estaciones comparte un anillo y el Token o estafeta pasa por todos los nodos sin importar si el paquete va dirigido o no a ellas. Caso similar ocurre con el FDDI.

En otros términos, el medio compartido tiene un ancho de banda definido y fijo que debe ser distribuido entre quienes quieran utilizar ese medio.

La consecuencia de utilizar estos medios es la consecuente reducción en la eficiencia de la transmisión, ya que a mayor número de usuarios o terminales la respuesta es lenta.

Por esta razón se crearon los medios conmutados. Un medio conmutado es aquel que designa un ancho de banda definido y único para cada conexión origen-destino, sin ser utilizado por nadie más. Para cada conexión debe establecerse este ancho de banda y se conoce como PVC ("Permanent Virtual Circuit"; circuito permanente virtual).

Con la utilización de los PVC's se garantiza un ancho de banda para cada conexión y por este medio no puede circular información de otros.

ATM, X.25 y Frame Relay utilizan esta filosofía y no acarrean los problemás de los medios compartidos.

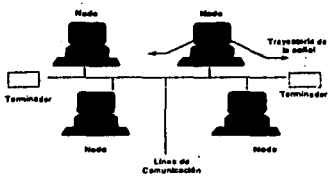
3.3.3. Protocolos de acceso al medio

El protocolo determina el método con lo que los nodos ganarán el acceso al cableado. Los más utilizados son:

a) *CSMA / CD*

Sus siglas significan "Carrier Sense Multiple Access with Collision Detection ; Acceso múltiple con detección de portadora y detección de colisiones". Este protocolo es utilizado junto con la arquitectura de bus lineal, en redes Ethernet (10 Base T) o Fast-Ethernet (100 Base T)

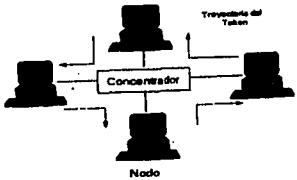
En este protocolo los nodos "escuchan" continuamente a la línea para saber si esta ocupada o no, y cuando esta se desocupa el nodo envía sus paquetes. En el caso de que dos nodos transmitan su señal simultáneamente, se presenta una colición que será detectada por los nodos, que esperaran un tiempo aleatorio para reintentar su transmisión.



b) *Paso de fichas ("token Passing")*

Este protocolo se utiliza en arquitectura de anillo modificado y doble anillo redundante, en el no se gana el acceso cuando se requiere, ya que los nodos desde su lugar deben esperar su turno para recibir la ficha (token), la cual se intercambia en forma de anillo.

Cuando un nodo obtiene la ficha cambia el primer bit para identificarlo como un paquete de datos, añade los datos y una dirección envía la señal hacia la corriente. Cada nodo de anillo checa si el paquete esta direccionado a él. Si no fuera así, el nodo retransmite el paquete. Cuando el nodo direccionado recibe el paquete, verifica que la información sea correcta. Copia los datos, marca el paquete como recibido y regresa el paquete original al anillo. El nodo transmisor remueve el paquete original y añade una ficha nueva.



c) *ATM*

ATM ("Asynchronous Transfer Mode" ; Modo de transferencia asincrónica) es un estándar muy reciente que define técnicas de alta velocidad, tanto para redes de área local (LAN) como para redes de área amplia (WAN),por esta razón esta a la expectativa de sus avances.

ATM es una técnica de red que usa un medio conmutado, es decir, se basa en la conmutación de paquetes. Puede ser instalado tanto sobre cable de cobre par torcido, como fibra óptica. Esto explica el por que ATM soporta velocidades de transmisión que varían desde los 25 MBits/s hasta 622 Mbits/s. En la actualidad se planea llevar esta velocidad hasta 2.48 Gigabits/s.

ATM tiene la característica de transmitirse de manera asíncrona, puesto que no utiliza marcos de informacións convencionales como las técnicas de redes locales. En cambio ATM crea celdas de información de tamaño fijo de 53 bytes, que son usadas para el encabezado. El resultado es la simplificación y la reducción de los costos del hardware; además de una gran flexibilidad.

ATM aprovecha al máximo la velocidad de un medio físico, puesto que no crea marcos de información con información de control de errores. la eficiencia de los medios físicos ha llegado a ser muy confiable y no es

necesario un control de errores tan intenso. Por otro lado, al tratar de obtener interoperabilidad entre ATM y otras técnicas de red, se necesitara de un mecanismo de conversión.

Debido a que ATM puede servir a todo tipo de configuraciones de red (incluso redes mundiales) y para distintos tipos de nodos y aplicaciones, es impredecible el tráfico transmitido, y por lo tanto, asincrono. Gracias a que el tamaño de las celdas es fijo, el retraso en ATM puede calcularse sin problemás. Al permitir ATM tener tan altas velocidades de transmisión, puede implantarse aplicaciones interactivas basadas en multimedia o audio y video digitalizados.

3.4 COMPONENTES

3.4.1 Concentradores inteligentes

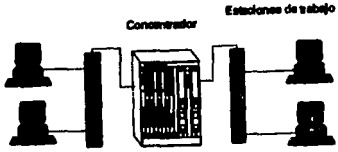
a) *Historia*

El primer concentrador para red surgió como una respuesta a los problemás de cableado existentes en las redes Ethernet con cable coaxial, en 1985 Xerox Corporation comenzó el desarrollo de lo que seria el primer concentrador para Ethernet.

En 1988 es el año en el que surge el primer concentrador comercial para Ethernet, fabricado por la compañía SynOptics Communications. Poco tiempo después se desarrollaron concentradores más sofisticados para soportar otros protocolos como Token Ring, FDDI y recientemente ATM.

b) *Definición*

Un concentrador inteligente es el punto central del cableado de una red, ya que aquí es desde y hacia donde fluyen todas las comunicaciones de una red.



c) *Elección de un concentrador inteligente*

Cuando la base de una red empieza a crecer, instalar un concentrador inteligente es la mejor opción que tiene los administradores para mantener un control adecuado. Actualmente las redes cuentan con una gran diversidad de tecnología instalada en diferentes localidades y a veces es difícil definir cuales son las necesidades reales de control. Una de las razones para elegir un concentrador inteligente es su capacidad de administración, ya que da control absoluto sobre los diferentes recursos y sistemás que se encuentra en la red. A continuación se presentan algunos criterios que se deben tomar en cuenta:

* Modularidad

Existen en el mercado una gran cantidad de fabricantes que ofrecen concentradores inteligentes básicamente se dividen en dos grandes grupos:

No modulares.- estos concentradores son utilizados para pequeños grupos de trabajo que pueden ser interconectados entre si y que soportan un sólo protocolo como Ethernet, Token Ring, FDDI, ATM.

Modulares.- estos son concentradores que nos permiten integrar en un solo chasis varios métodos de acceso y múltiples protocolos como Ethernet, Token Ring y FDDI; y que además permiten integrar dispositivos adicionales para dar interconectividad a la red y servicios adicionales como puentes, ruteadores, conmutadores,

conexiones a host, servidores en el mismo chasis, etc. Estos concentradores trabajan a través de módulos que cumplen una función especifica.

• Confiabilidad

Existen redes que manejan aplicaciones altamente criticas para una empresa y que por ninguna razón deben detener su funcionamiento. Hay concentradores que ofrecen un grado de confiabilidad superior a otros dispositivos de respaldo, algunos de estos son: fuentes de poder redundantes, backplane redundante, ventiladores redundantes, capacidad de desmontar y montar, módulos en tiempo real, administración, autosupervision y diagnóstico.

• Jerarquía

Es importante definir desde un principio la jerarquía de los concentradores en la red. Es decir, diseñar la red tomando en cuenta el tráfico que va a fluir. Esto servirá para escoger el concentrador adecuado y localizarlo en el punto necesario; ya que existen concentradores que pueden administrar a otros.

• Administración

Para la administración de una red, la Organización Internacional de Estándares ha categorizado las funciones de administración de redes de la siguiente manera: administración de fallas, administración del funcionamiento, administración de la configuración, administración de cuentas, administración de seguridad.

Los concentradores inteligentes tiene la habilidad de recolectar información y comunicarla a través de los protocolos de administración de la red, lo que permite identificar y corregir fácilmente fallas. La profundidad con la que un concentrador inteligente puede administrar una red dependerá de sus especificaciones y caracteristicas.

* Velocidades del backplane

El backplane es el elemento de un concentrador modular que sirve como interfase de conexión entre módulos. La velocidad de transferencia de datos entre dos nodos que pertenecen a dos módulos distintos depende de la velocidad del backplane.

Algunos de los concentradores emplean un backplane de alta velocidad, ofreciendo velocidades que van desde Megabits a gigabits por segundo. La velocidad del backplane es uno de los factores importantes a considerar cuando se selecciona un concentrador inteligente que dará servicio a redes grandes.+

* Segmentación de la red

Las redes son cada vez más grandes y complejas. Aunque su finalidad es que todos los usuarios tengan acceso a todos los recursos de la red, es necesario separar el tráfico en segmentos.

Para lograrlo es necesario aplicar métodos de segmentación, es decir, permitir que el tráfico fluya localmente en un segmento de usuarios comunes evitando que se mezcle con el tráfico de otro segmento de usuarios comunes. Solo se debe permitir el paso ocasionalmente a la información de un segmento a otro cuando vaya dirigida a ese segmento.

Actualmente existen varios métodos para segmentar el tráfico en una red como son: conmutar, hacer puentes y ruteo. Esto métodos se pueden realizar dentro de los concentradores inteligentes o bien fuera de ellos con dispositivos que cumplan funciones específicas, como es el caso de los ruteadores.

* Apego a estándares

Todos los concentradores inteligentes deberán apegarse a los siguientes estándares:

a) *Ethernet*

Velocidad de transmisión soportada: 10 Mb/s

Estándar: IEEE 802.3 tipo 10Base-T (Cable UTP)

IEEE 802.3 tipo 10BASE2 (Cable Coaxial)

IEEE 802.3 tipo AUI

IEEE 802.3 tipo FOIRL (Fibra Optica)

b) *Token-Ring*

Velocidad de transmisión soportada: 4MB/s o 16MB/s

Estandar: IEEE 802.5 Token-Ring.

c) *FDDI*

Velocidad de transmisión soportada: 100 MB/s

Estándar: ISO 9314-1 FDDI Physical Protocol Standar

ANSI FDDI X3T9.5 station mangement specification

ANSI Draft Twisted-Pair Physical Media Dependent specification.

Velocidad de trasnmision soportada: 155.52 Mb/s

Estándar: en proceso

ATM Forum 155 Mb/s SONET/SDH

d) *Fast Ethernet* 100 Base T

Velocidad de transmisión soportada: 100 MB/s

Estándar: 100Base T IEE 802.3 U

Soporta marcos de informacións Ethernet

e) 100 VG AnyLAN

Velocidad de transmisión soportada: 100 MB/s

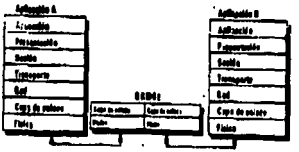
Estándar: IEEE 802.12

Soporta marcos de informacións Ethernet y Token Ring.

3.4.2 Puentes (Bridges)

Los puentes (bridges) son dispositivos que conecta dos redes LAN para crear lo que aparenta ser una sola red. Los puentes revisan si la dirección asociada a cada paquete de información es la correspondiente al otro segmento de red, si lo es, el puente pasará el paquete a dicho segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento actual no pasará dicho paquete.

Los puentes son dispositivos que incrementan la producción de una LAN al filtrar servidores entre segmentos de la red definidos con base en direcciones de hardware. Opera en la capa de enlace de datos del modelo OSI.



Si se tienen múltiples dispositivos conectados a una LAN de tal forma que por su número y por la demanda de servicios de la red impactan negativamente su eficiencia, se necesita dividir la LAN en segmentos e interconectarlos mediante puentes.

Los puentes usualmente interconectan medios iguales de acceso (Ethernet con Ethernet y Token Ring con Token Ring), pero por definición pueden conectar medios diferentes.

En la capa de enlace de datos, las señales en el cable están organizadas en marcos de información llamados "Media Acces Control; Control de acceso al medio " (MAC). Los encabezados de los marcos de información contiene información acerca de las direcciones de origen y destino del servidor. Estas direcciones se conocen como direcciones MAC.

Los puentes tienen la capacidad de filtrar tráfico entre segmentos de LAN basados en estas direcciones. Filtrar es la capacidad del puente de transmitir a un determinado segmento sólo los marcos de informacións que tengan por destino un dispositivo en este segmento en particular. Esta capacidad incrementa la producción de una LAN segmentada.

Los dispositivos que se encuentran en una LAN segmentada bajo este ambiente transmite sus marcos de información como si todos los dispositivos estuvieran en una sola LAN, es decir, el dispositivo que transmite, direcciona el marco de información de la MAC directamente al dispositivo destino. No así al puente, que toma los marcos de información y decide a donde enviarlos.

Cuando se diseña una LAN con puentes, una buena regla es seguir un tráfico 80/20, 80% del tráfico debe ser local (en el segmento) y 20 % pasar entre segmentos.

Los puentes trabajan independientemente de las capas superiores a la capa de enlace de datos del modelo OSI. Esto significa que no importa que tipo de protocolos sean utilizados en el área de datos del marco de información, ya que estos datos no afectan la forma en que los marcos de información son filtrados.

Existen tres tipos de puentes:

• *Transparente bridge (puentes transparente)* .- estos puentes son muy populares ya que son del tipo conéctese y úsese. Esto significa que requieren poca cooperación del usuario, que es en todo caso, instalarlo para operar. Se llaman así porque los dispositivos conectados a los segmentos de la LAN transmiten sus marcos de información dirigidos al dispositivo destino como si este estuviera en la red sin segmentar. El dispositivo que envía no sabe que el dispositivo destino esta o no en otro segmento; o que un puente o una serie de ellos se encuentran entre los dos dispositivos.

• *Source Routing Bridges (puente de ruteo fuente)* .- estos puentes y su método de ruteo difieren del puente transparente en que no mantienen una tabla de filtrado. En cambio cada dispositivo en una red de este tipo mantiene su propia tabla de rutas hacia los dispositivos con los que se comunica. Esta tabla de rutas en los dispositivos, contiene información que describe el camino para llegar al dispositivo destino. Esta información se incluye en el área de datos del marco de información, la cual es insertada por el dispositivo. El puente transmite o filtra los marcos de informacións basados en esta información.

• *Source Routing Transparent Bridges(Puente transparente de ruteo fuente)* .- este tipo de puentes son una implementaron que soporta las especificaciones de los dos puentes ya mencionados. Actúa como un puente de ruteo fuente para aquellos marcos de informacións que tienen información de ruteo y como puente transparente para los demás marcos de informacións al filtrarlos con la tabla. Estos puentes son útiles en ambientes donde sólo algunos dispositivos necesitan comunicarse con equipos IBM.

3.4.3 Protocolos LAN

Un protocolo es el lenguaje a través del cual se comunican dos dispositivos. Es una serie de reglas que ambos, transmisor y receptor deben cumplir para entenderse. Existen muchos protocolos que han sido desarrollados por universidades, compañías, organizaciones, laboratorios y hasta aficionados.

Dentro de esta enorme variedad de protocolos es donde las organizaciones de estándares juegan un papel determinante. CCITT ("Consultive Comitee for International Telegraphy and Telephony" ; Comite Consultivo Internacional de Telefonía y telegrafía"), ISO ("International Organization for Standarization" ; Organización Internacional de Estandarizaciones) e IEEE ("Institute of Electrical and Electronics Engeneers" ; Instituto de Ingenieros Eléctricos y Electricistas) son organizaciones que regulan la estandarizacion de los protocolos.

Los protocolos LAN se pueden dividir en dos categorías fundamentales, que son:

Capa 2	*Capa 4.....Capa 3*
Acceso al medio	Transporte...../.....Red
CSMA/CD (Ethernet)	TCP/IPX
Token Ring	SPX/IPX
FDDI	DECNET
ATM	Apple Talk
	OSI

De cualquier forma, un protocolo juega reglas para construir paquetes de información que pretenden llegar a su destino y así establecer una comunicación.

Hablando genéricamente, un paquete de información se forma de campos de información que tienen un significado y función diferente. Todos estos campos los podemos agrupar en dos divisiones: el encabezado o header y los datos.

El encabezado de un paquete contiene, dentro de sus campos, información acerca de quien es el origen, cual es el destino, el tipo de información que lleva, la longitud del paquete, la importancia del paquete, la vida del paquete, banderas de control, campos de verificación y otros. Los datos son propiamente la información que debe llevarse de un punto a otro.

Según el protocolo, los paquetes que genera pueden tener más o menos campos en el encabezado de los que se han mencionado, esto atendiendo al propósito para el cual fue diseñado.

3.4.4 Conmutadores

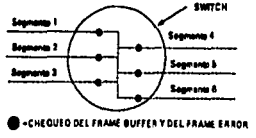
Un conmutador (switch) local es un dispositivo inteligente que permite la interconexión de redes de uno o diferentes protocolos, dando capacidades de segmentación en las redes.

Existen varios tipos de conmutadores, los más comunes son:

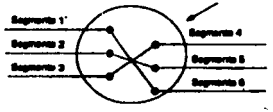
a) *Conmutadores Ethernet (Switches Ethernet)*

Los conmutadores Ethernet tuvieron su desarrollo inicial en 1991, como una forma de segmentar y hacer más eficiente la comunicación entre diferentes segmentos de Ethernet. Actualmente los diferentes fabricantes de conmutadores utilizan diversas técnicas de conmutación siendo las principales :

* *Store and Fordward switch (conmutador de almacen y transmisión)* .- esta técnica maneja áreas de almacenamiento temporal (buffers) para cada puerto y cada marco de información que se desea enviar, es detenido y se verifica los posibles errores, una vez que ha sido verificado entonces se envía a su dirección destino.

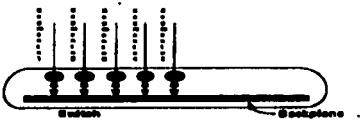


* *Cross Bar Switch* (conmutador de barra cruzada).- en esta técnica los marcos de información son enviados de una dirección origen a una dirección destino sin ninguna reserva, es decir, no se realiza ninguna verificación de errores.



●=RECONOCIMIENTO DE LA DIRECCION DEL FRAME Y ENTRADA DE FIFO'S

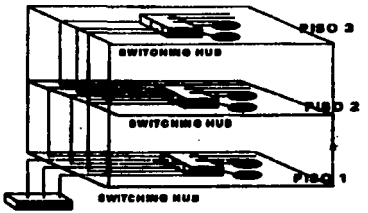
* *Cell backplane switch (conmutador de celda para backplane).*- en esta tecnología los marcos de información son segmentados y rensamblados utilizando métodos como "fast cell switching" (rápida conmutación de celda) para seleccionar la dirección destino.



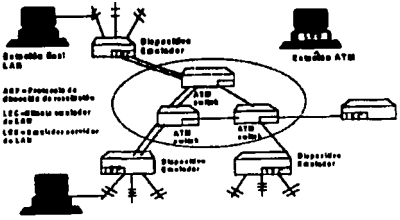
●=SEGMENTACION DEL FRAME Y BUFFER DE SALIDA

b) *Conmutadores para ATM (Switches para ATM*

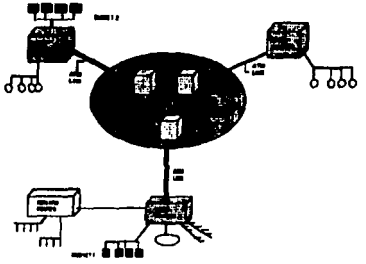
* Conmutación LAN (*LAN Switching*) .- es una forma de puente que se desarrolla en la capa 2 del modelo OSI ofrece un ancho de banda total de 10 o 16 Mbps a cada puerto.



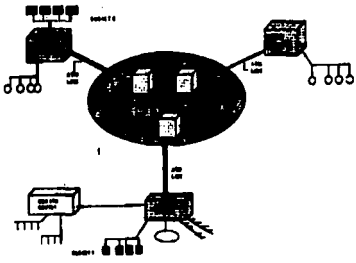
* *Emulación LAN (LAN Emulation)* .- define 2 componentes principales de software. El cliente de emulación LAN (LEC, LAN Emulation Client) y el servidor de emulación LAN (LES, LAN Emulation Server). El LEC actúa como un nodo ATM, convierte las direcciones MAC en direcciones ATM, cuando el LEC desea lanzar un marco de información a través del dispositivo ATM hacia un nodo de red, este envía al LES una dirección MAC a ATM bajo el protocolo de resolución de direcciones (ARP, Adress Resolution Protocol). El LES responde con una dirección ATM del LEC que fue ligado al nodo objetivo. El LEC que origino la comunicación establece posteriormente, un circuito virtual switcheado (SVC, Switched Virtual Circuit) de ATM con el nodo objetivo LEC. los marcos de informacións de MAC son entonces convertidos en celdas ATM on una segmentación estándar y reensamble (SAR) en cada LEC.



• *Rango de Ruteo (Edge Router).-* cada rango de ruteo corre un ARP (Adress Resolution Protocol) especial que hace posible localizar subredes virtuales. Para encontrar una subred IP, el dispositivo del rango de ruteo que originó la comunicación lanza un marco de información en ARP hacia todos los demás dispositivos de rango de ruteo, estos tomarán el IP, el ruteador remoto entonces responderá con su dirección ATM, y se establecerá un circuito virtual. Las subredes virtuales pueden darse de alta, a través de múltiples segmentos de red local. Todo esto por medio del backbone.



• *Ruteador Virtual (Virtual Router).-* consta de un ruteador central y de un número de conmutadores Multicapa (Multilayer Switches). Cuando un nodo de la red trata de establecer una sesión a través del conmutador multicapa, el ruteador intercepta el primer paquete, localiza el nodo objetivo y crea un camino entre el origen y el destino, posteriormente envía una dirección ATM a quien originó en la conmutación multicapa.



3.4.3 Ruteadores

El ruteador es similar al puente sólo que opera a un nivel diferente, este requiere que cada red tenga el mismo sistema operativo. Con un sistema operativo en común el ruteador puede ejecutar funciones más avanzadas, como conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring, así como determinar la ruta más eficiente para el envío de datos en caso de haber más de una ruta.

Los ruteadores tienen acceso a la información de las tres capas inferiores OSI (Física, enlace de datos y RED). La información de la capa 3 generalmente incluye lo que se llama un direccionamiento lógico de la red. El direccionamiento físico no es asignado por el administrador de la red, mientras que el direccionamiento lógico si lo puede ser. Esta es la diferencia básica entre un puente y un ruteador

El administrador puede usar los direccionamientos lógicos para asociar un grupo de equipos con algunas características en común. Estas direcciones proporcionan la flexibilidad que un direccionamiento físico no tiene, sencillamente estos pueden ser agrupados jerárquicamente y cambiarse más fácilmente.

Los ruteadores envían información a través de la parte interna de la red usando información de direcciones lógicas en lugar de físicas. Las subdivisiones de una red lógica a menudo son llamadas subredes. Una subred puede o no, trazarse (mapearse) directamente a un solo segmento físico.

Los ruteadores usan también uno ó más algoritmos de ruteo específicos para calcular el mejor camino a través de la parte interna de la red. Los caminos pueden calcularse en términos de tiempo real (dinámicamente), a fin que puedan ajustarse constantemente a las condiciones cambiantes de la red o establecerse en rutas estáticas capturadas por el administrador.

Los protocolos de ruteo dinámico difieren en los factores métricos que ellos consideran cuando realizan el cálculo de la mejor ruta, por ejemplo, un protocolo de ruteo puede determinar el mejor camino basándose en el menor número de saltos hacia su destino.

3.4.6 Multiplexores

Los ruteadores permiten conectar redes locales usando un enlace remoto, pero si existe la necesidad de compartir ese enlace entre distintos dispositivos, se requiere de un equipo que permita que estos dispositivos tengan acceso a ese medio sin que noten la presencia de este equipo. Los multiplexores y conmutadores realizan esta función.

Los multiplexores toman múltiples flujos de información y los coloca en un único medio físico de transmisión, mientras que los conmutadores pueden tomar información previamente multiplexada (junto con otras fuentes de información), reordenar la información y entregarla en otra posición hacia un multiplexor de salida.

• *Multiplexor por división de frecuencia (FDM).*- múltiples señales analógicas pueden ser multiplexadas en un mismo cable modulado, cada una de ellas en una frecuencia portadora distinta, siendo muy útil para transmisiones telefónicas. Con el paso del tiempo se empezó a utilizar para la transmisión de datos, pero con malos resultados, principalmente por el ruido, distorsión e interferencias generadas entre las frecuencias portadoras. Su ventaja fundamental es que permite la transmisión ininterrumpida por cada canal, sin embargo, si no es utilizado ese canal el ancho de banda se desprecia.

• *Multiplexor por división del tiempo (TDM).*- con la introducción de señales digitales fue posible dividir temporalmente el ancho de banda disponible. Cada canal utiliza la troncal completa por un periodo corto de tiempo.

• *Multiplexor estadístico por división de tiempo (STDM).*- opera igual que el TDM, pero con la ventaja de que puede asignar cada segmento de tiempo al canal que lo necesite. Esta ventaja permite obtener un 200% de rendimiento sobre una troncal con tecnología TDM.

3.4.7 Compuertas (Gateways)

Gateway o compuerta lógica permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Podría tenerse por ejemplo, una LAN que consiste de computadoras compatibles con IBM y otra que consiste en computadoras Machinstosh. En este caso, un gateway permitiría que las computadoras IBM compartan archivos con las Machintosh. Este tipo de compuerta permitirá también que se compartan impresoras entre las dos redes.

3.4.8 Transmisores/repectores (Transceivers)

El transmisor/receptor tiene entre sus funciones principales :

- Función de transmisión.- transmite una serie de datos del nodo o equipo terminal de datos a un medio físico.
- Función de recepción.- recibe los datos del medio físico para el equipo de terminal de datos.
- Presencia de colisiones.- si un MAU("Media Access Unit" ; Unidad de acceso al medio) esta transmitiendo, este detectará la presencia de dos o más MAU's que están también transmitiendo señales a través de un medio físico. Si no transmite el MAU puede detectar la presencia de dos MAU's transmitiendo.
- Función de balbuceo.- tiene la capacidad de autointerrumpirse por el cual el MAU puede inhibir la transmisión de marcos de información adicionales al medio después de percibir que algún equipo de terminal de datos esta transmitiendo marcos de informacións inválidos.
- Función de mensajería.- un MAU envía mensajes a la capa física del equipo terminal de datos acerca del estado en que se encuentra. También envía mensajes de error cuando siente que hay transmisiones múltiples .

3.5 Ventajas de las redes locales

- Algunos estudios afirman que el 80% de los requerimientos de procesamiento en las aplicaciones más comunes se resuelven en un entorno de 70 metros de la ubicación del usuario, y otro 10%, dentro de los 800 metros. Si no atendemos a estas cifras, lo que se entiende es que se tiene cierto riesgo, el 90% de los requerimientos de procesamiento, puede ser resultado dentro de una LAN. Esto, de por sí, sería una gran ventaja de la utilización de redes locales.

- Es indudable que el poder compartir recursos trae mayores posibilidades desde el punto de vista de las aplicaciones así como también disminuye los costos por usuario conectado.

* Compatibilidad de equipos. En una LAN que tenga cierta flexibilidad a nivel de interconexiones, es posible juntar equipo de diferente tecnología, proveedor, aplicación, etc.

* Procesamiento distribuido. La posibilidad de tener unidades redundantes, no depender de un único elemento central, disponer de cierto grado de independencia a nivel usuario, poder procesar en el lugar donde se originan los datos y se toman las decisiones finales, etc.

* Aplicaciones complementarias o de valor añadido. Las comunicaciones entre terminales, el acceso a bases de datos y documentación útil, el soporte de correo electrónico, etc.

* Ventajas comparativas con otros equipos de conexión. Velocidades mayores, menor tasa de error, distancias mayores, transmisión simultánea de información de distinta naturaleza.

* Distribución física del Hardware. Las LAN's permiten optimizar la disposición de los equipos, mejorando la interrelación entre el hombre y la máquina, los requerimientos ambientales, reduciendo costos de instalación, volviendo estéticamente mejores los lugares de trabajo.

* Simplicidad y flexibilidad de modificaciones de configuración. En muchas LAN's, las altas y bajas de elementos de la red no afectan al resto de los usuarios ni implican cambios en el software de control.

3.6 Aspectos en la evaluación de redes locales

Una red local es simplemente un mecanismo de transporte de datos, y no necesariamente implica una solución a los problemás existentes en las aplicaciones, por lo tanto, un correcto análisis de las necesidades del usuario, hecho al comienzo, puede extender el ciclo de vida de la red, limitar los costos de mantenimiento y

asegurar un servicio más adecuado a los usuarios. Algunos de los aspectos a considerar en la implantación de una red local son los siguiente:

- Los tipos de datos a transportar por la red
- Tipo de dispositivos y que cantidad de estos se van a interconectar
- Topología a utilizar
- Características ambientales del lugar donde se instalará la LAN (ductos, cableado,etc.)
- Dependiendo del tipo de procesamiento ver los requerimientos en cuanto a tiempos de respuesta y rendimientos del sistema, evaluar el movimiento de los datos según su tipo, volumen, destino y prioridad de entrega
- Tipos de compuertas de pasaje a otras redes
- Establecer niveles de confiabilidad requeridos, tanto en los enlaces, como los dispositivos a conectar.
- Establecer las holguras que se dispondrán en lo que respecta a volumenes, tiempos y expansión.
- Facilidades de reconfiguración ofrece la red.
- Condiciones técnicas y económicas del mantenimiento de la red
- Garantía que ofrece el proveedor del sistema

Una forma de plantear los principales factores que determinan en la práctica un tipo de red local, es el siguiente: nombre, velocidad, técnica de acceso, técnica de transmisión, técnica de conmutación, topología, tecnología, capas, compatibilidad con otros modelos y proveedor.

Aquí se concluye este capítulo, en el cual se deserrollaron las características principales de una red local (LAN), así como también se definieron cada uno de los componentes y sus funciones principales de los elementos que conforman una red.

4. EL CONTROLADOR LATTISNET

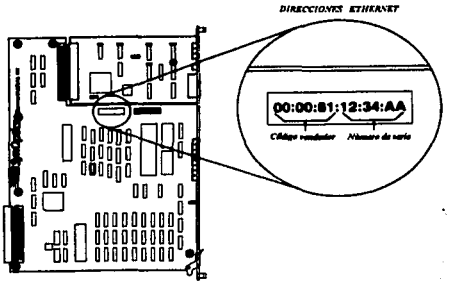
El controlador Lattisnet es un dispositivo que sirve como centro de control de una red con topología tipo estrella. También se puede referir como un dispositivo que contiene múltiples módulos de equipos de redes, y son estos módulos los que se describen en este capítulo.

4. 1 FORMATO DEL MARCO DE INFORMACION

El formato de un marco de información o paquete Ethernet contiene seis campos, los cuales se describen en la siguiente tabla:

CAMPO	NUMERO DE BITS	
Preamble (Preámbulo)	64	Establece sincronización de bits y condiciones del transmisor/receptor; terminados con la secuencia 10101011
Destination Address (dirección destino)	48	Direccionamiento jerárquico: la dirección consiste de un dispositivo ID y una red ID
Source Address (dirección fuente)	48	Direccionamiento jerárquico: la dirección consiste de un dispositivo ID y una red ID
Type (Tipo)	16	Tipo Ethernet FTP: datos, admisión, abortar, terminar, repetir
Data (dato)	368 a 12000	46 a 1500 bytes (unidades de 8-bits)
CRC	32	Checar redundancia cíclica para detectar errores que ocurren durante la transmisión

4.2 DIRECCIONES MAC

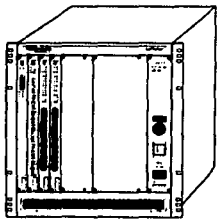


Las direcciones fuente y destino incluidas en el marco de información Ethernet son direcciones MAC ("Medium Acces Control" ; Control de Acceso al Medio). Una dirección MAC es un código del equipo de hardware y es referido como la dirección de hardware. Los tres bytes iniciales, o las seis posiciones hexadecimales de una dirección MAC, contiene el "código del vendedor". Este código del vendedor es una cadena de números que el manufacturador obtiene de el IEEE ("Institute of Electrical and Electronic Engineers" ; Instituto de Ingenieros Eléctricos y Electricistas). Cada compañía construye sus dispositivos que serán direccionados sobre una LAN y las cuales deben obtener sus códigos de vendedor directamente de IEEE. Esto asegura que no se duplicarán direcciones. El código de vendedor de Lattisnet SynOptics es 000081.

El segundo componente de la dirección de hardware es la dirección asignada del vendedor. La combinación del código de vendedor ordenada y el producto generado o número de serie garantiza que no haya duplicidad de direcciones de hardware sobre una LAN.

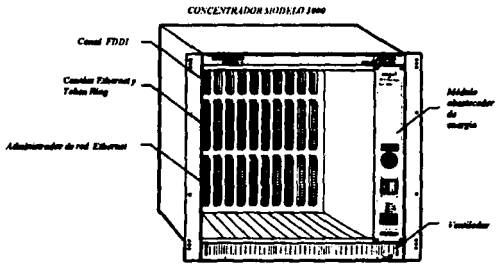
4.3 CONTROLADOR LATTISNET SYNOPTICS SERIE 3000

El controlador lattisnet Ethernet Serie 3000 actúa como un repetidor, transmite una señal recibida de alguna estación o controlador a todos los otros canales que se encuentren conectados. Este controlador también desempeñan las funciones de detección de colisiones, protección de balbuceos en la señal (basura en la transmisión) y extensión de segmentos.



Los componentes del controlador Modelo 3000 consiste de lo siguiente:

* Una canal Ethernet A con división de canales
* Administradora de red.
* Un módulo abastecedor de energía.
* Un bus FDDI opcional
* Token Ring opcional y un bus de canal Ethernet B estándar.
* Ventilador

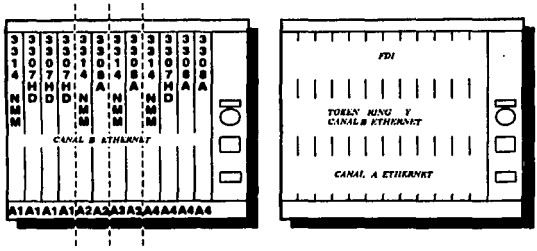


4.3.1 Abastecedores de energía

El controlador modelo 3000 tiene un ventilador y uno o dos módulos abastecedores de energía preinstalados los cuales son el modelo 3002 460-watt. El módulo abastecedor de energía 3002 puede manipular todos los diferentes tipos de voltajes necesarios para Ethernet, Token Ring y FDDI . Ver figura A del apéndice..

El controlador tiene un led el cual indica si la unidad esta recibiendo energía, cuando el led se encuentra en amarillo indica que uno o más de los ventiladores fallan o se encuentran muy bajos de energía. .

4.3.2 Multisegmento del backplane



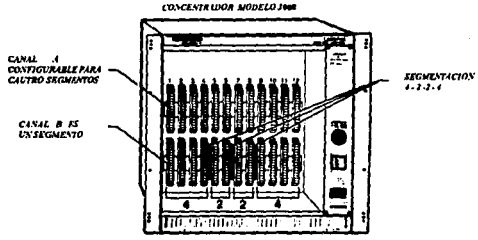
Entre las características que tiene el multisegmento del backplane se tiene:

* En el se conectan módulos Ethernet y módulos abastecedores de energía
* Contiene una interfase de administración de red
* Contiene dos canales Ethernet; algunos modelos incluyen token ring y FDDI.

Los módulos Ethernet del sistema 3000 se conectan a través de un conector de 96 pins al backplane del controlador.

El controlador modelo 3000 incluye un backplane con compatibilidad entre Ethernet y Token Ring. Con este backplane el mismo controlador pueden simultáneamente operar módulos pertenecientes a una red Ethernet a 10 Mb/s y módulos de dos red token ring a 4 o 16 Mb/s y tres vías FDDI (en el modelo 3000-05). Las redes pueden ser operadas independientemente de cada una y pueden ser conectadas juntas lógicamente con alguna combinación a través de uso de puentes o compuertas lógicas (gateways).

4.3.3 Segmentación del backplane



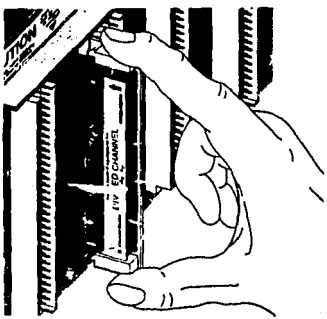
El backplane del controlador tiene dos canales Ethernet, llamados canales A y B. El *canal A* reside en la fila de conectores en la parte alta del backplane. Usando las divisiones de canales físicas, el *canal A* puede ser dividido en cuatro segmentos, cada uno de los cuales es asociado con una serie de ranuras particulares. Los módulos de ranuras pueden estar unidos o separados por divisores de canal para crear una variedad de configuraciones. De izquierda a derecha, con todas las secciones divididas en el *canal A*, sección A1 compuesta de cuatro ranuras, sección A2 y A3 incluyen dos ranuras respectivamente y la sección A4 incluye cuatro ranuras. Esto es llamado *segmentación 4-2-2-4.*

El *canal B* reside en la segunda fila de conectores y es el quinto segmento Ethernet. Este incluye a una ranura en el canal 12 al controlador. El canal B utiliza el conector DIN 96-pin como el del conector token ring. Usando Ethernet en aquel canal no causa interferencias con la operación token ring.

Estos canales no interfieren con algunas red token ring o FDDI que pueda existir en el controlador.

4.3.4 Divisor de canal

El divisor de canal es un módulo pequeño equipado con dos conectores de 25 pins. La parte de arriba del canal divisor es de color azul y etiqueta blanca que apunta a las funciones de los dos conectores. Cuando el divisor es instalado con las fechas del lado "Continuos" hacia el backplane, dos segmentos Ethernet adyacentes son unidos. Cuando este es instalado con las flechas del lado "Divided" apuntando hacia el backplane, el divisor de canal segmenta los ranuras sobre un mismo lado de aquellos del otro lado. El divisor de canal puede ser removible para configurar el controlador en número y tamaño de segmentos deseados.



Los divisores de canal son localizados entre las ranuras 4/5, 6/7 y 8/9 en el modelo 3000. Todos los divisores de canal deben ser instalados y reconfigurado cuando el controlador este apagado.

4.3.5 Segmentación y canales del controlador

El controlador lattisnet de la series 3000 soporta según su nomenclatura:

* 3000N -dos canales Ethernet, arriba de cinco segmentos

* 3000NT - dos canales Ethernet y dos token rings
* 3000NTR - dos canales Ethernet, dos token rings y abastecedores de energia redundantes
* 3000S - dos canales Ethernet, dos token rings y tres vias FDDI
* 3000SR - dos canales Ethernet, dos token rings, tres vías FDDI, abastecedores de energía redundantes

4.3.6 Nomenclatura del modelo

El número de módulo tiene la forma 3WXY, donde:

* 3 indica Módulo Sistema 3000
* W indica el tipo de LAN o protocolo
* X indica el tipo de módulo
* Y indica el tipo de medio

La siguiente tabla muestra el esquema de numeración del modelo 3000:

3= Physical layer	3 = Ethernet	0 = host	1 = ThinNet
	5 = Token ring	1 = network management	2 = STP
	9 = FDDI	2 = bridge	3 = AUI
		3 = retiming	4 = fiber optic
		5 = Ring In / Ring Out	5 = UTP
		8 = router	7 = 50-pin 10BASE-T
		9 = terminal server	8 = RJ-45 10BASE-T

4.4 MODULOS DEL CONTROLADOR LATTISNET SYNOPTICS SERIE 3000

Los módulos huespe (host) Ethernet son instalados en las ranuras del controlador Sistema 3000. Los módulos pueden ser un "host" o huesped, un administrador de red, un puente, o ruteador. Ver figura B del apéndice. Los módulos tiene como característica :

- Transmisión de datos a 10 Mb/s sobre UTP, STP, coaxial y fibra óptica.
- Autodivisión por puerto de red: desabilita conexiones en eventos de colisiones excesivas (condiciones de error) en nodos o roturas de enlace. Los puertos son automáticamente reconectados una vez que la falla es corregida.
- Pruebas de integridad de enlace: monitorea los datos recibidos del UTP y determina la integridad del segmento de enlace.
- Detección de autopolaridad y corrección para las inversiones de señal de los datos recibidos del UTP.
- Se tiene un sistema administradora de red con pormenores del puerto y nivel de monitoreo por tarjeta y capacidades de control. Identificación de módulos e información de configuración es automáticamente presentada en el consola de control de la administradora de la red en tiempo real usando interface gráfica.
- En la parte de enfrente se tiene un panel de LED's que indican el status de las tarjetas, división y actividad de administración de la red.

4.4.1 Transmisor/repector Lattisnet

El transmisor/receptor (Transceiver) lattisnet se utilizan para conectar una estación o nodo a un controlador en un sistema de cableado utilizando el estándar IEEE 802.3 en un AUI.

El transmisor/receptor es externo al nodo. Cada tipo de cableado tiene un transmisor/receptor correspondiente:

• Transceiver modelo 502A, es utilizado para cable UTP.

• Transceiver modelo 504A, utilizado para cable de fibra óptica con conectores ST.

• Transceiver modelo 505, utilizado para cable UTP (pre-10BASET)

• Transceiver modelo 508B y 928 para instalaciones UTP operando bajo el estandar IEEE 802.3i

• Transceiver modelo 518, para estaciones Macintosh.

El transmisor/receptor tienen dos led's que indican lo siguiente:

• Led link status (led de estado de enlace).- este led se encuentra encendido cuando el transceiver está conectado a un módulo y que haya conexión del cable al módulo apropiado.

• Led de prueba SQE.- este se encuentra encendido cuando el transceiver detecta algún error de transmisión o la conexión no es la apropiada.

4.4.2 Módulo Modelo 3308A 10Base-T Host

Este modelo tiene las siguientes características (Ver figura C del apéndice) :

- 12 Puertos compatibles con IEEE 802.3i para conexiones de par trenzado
- Conectores RJ-45 hembras, los conectores machos RJ-45 del cable UTP se conecta directamente a puerto del módulo.
- Conexiones que protegen el cable par trenzado usando el modelo 822 10 BASE-T adaptador tipo 1.
- Modulo e indicadores de puertos, como se muestra en la tabla siguiente.

Modulo			El módulo esta recibiendo energía
LEDS			
			Si un módulo administrador de red (NMM) es instalado, este led indica que la comunicación al NMM esta funcionando apropiadamente y el administrador de la red no ha detectado fallas en el módulo. Si el software del administrador de la red no es cargado al NMM en aproximadamente un minuto después de haberse encendido (esto es, el Led de NMM ON Line esta destellando) el estado del LED del módulo estará apagado.
	Parte	ámbar	El módulo ha sido particionado del backplane por el administrador de la red.
	NM Cmrl	ámbar	Uno o más puertos son controlador por el administrador de la red
Port	Link Status	verde	El módulo es conectado a un transmisor/receptor o la tarjeta de interfase de
LEDS			red reconoce el dispositivo IEEE 802.3i 10BASE-T.
		ámbar	El puerto ha sido particionado por un excesivo número de colisiones consecutivas, o el puerto ha tenido una larga señal de colisión o el puerto ha sido particionado por el administardor de red.
		apagado	Estado del enlace

4.4.3 Módulo Modelo 3307 50-Pin 10Base-T Host

Este módulo tiene las siguientes características (ver figura D del apéndice):

- 12 puertos para conexiones de par trenzado (UTP) a dispositivos compatibles 802.3i 10Base-T
- Interfase de administrador de red, LNMS versión 3.2 o más reciente y todas las versiones de UNIX.

4.4.4 Módulo Modelo 3307HD 10Base-T Host

El modelo 3307HD tiene las siguientes características (Ver figura E del apéndice):

- 4 puertos para conexiones UTP con dispositivos compatibles 802.3i 10 BASE-T. Esto permite una configuración por arriba de 264 puertos en el modelo 3000 o 72 puertos en el modelo 3030.
- Dos conectores D hembras 50-pin
- Protector de intercambio rápido "Hot-swap ", el cual permite insertar y quitar el módulo de algún controlador

estando encendido.

* Manual o controlador de administración de red seleccionando entre los canales A y B.
* El modelo 3307HD requiere un NMM que soporte canales A y B para una apropiada operación.
* Módulo e indicadores con LEDs con las mismas funciones como los otros módulos 10BAse-T. Adicionalmente indicadores de LED que indican lo siguiente:

Canal de LEDs	**A**	**verde**	**El módulo es conectado a la fila del canal A de los conectores del backplane**
	B	**verde**	**El módulo es conectado a el canal B en la segunda fila de los conectores del backplane**
MDI-X	**Enable**	**verde**	**El puerto 24 es conmutado fuera del conector Telco y ahora es un conector RJ-45**

4.4.5 Módulo Modelo 10Base2 Host

Los módulos 10BASE2 para los controladores 3000 son los módulos modelos 3301, 3301-75 y 3301-93. Ver figura F del apéndice . Cada módulo contiene lo siguiente:

* Ocho puertos BNC, cada uno soportando 29 estaciones.
* Longitud máxima por segmento de enlace: 185 m par módulo modelo 3301 y 100 m para modelos 3301-75 y 3301-93.
* Cada puerto es terminado internamente (50 ohms) y aterrizado.
* Interface administrador de red: cada módulo contiene un controlador estación a estación topología estrella para estaciones equipadas con tarjetas adaptadoras compatibles o transceivers
* Módulo e indicadores de puerto con LEDs, como se muestra a continuación:

Modulo	Status	verde	El módulo esta recibiendo energía.
LED			Si el administrador de red (NMM) esta instalada, este LED indica que la comunicación al NMM esta funcionando correctamente y el administrador de red no ha detectado error en el módulo.
	Part	**ámbar**	**Este módulo ha sido particionado del backplane por la administradora de red.**
	NM CNTRI	ámbar	Uno o más puertos son controlados por la administradora de red.
	LinkStatus	verde	Si la administradora de red particiona el puerto, el LED será forzado a apagarse, sin hacer caso del estado del segmento de cable coaxial.
PortLED	PartStatus	ámbar	El módulo ha sido particionado del backplane por la administradora de la red, o autoparticionamiento por haber un número excesivo de colisiones.
			Trozamiento del cable coaxial causa al puerto se autoparticione después de 31 colisiones consecutivas.

4.4.6 Módulo Modelo 3302 STP Host

Este modelo es usado para correr Ethernet sobre nuevas o existentes UTP. Ver figura G del apéndice. Este módulo tiene las siguientes características:

- Compatibilidad con cableado IBM
- Seis puertos para conexiones UTP a transmisores/receptores s SynOptics o tarjetas de interfase de red
- Estado de funcionamiento por puerto
- Autoparticionamiento por puerto, las cuales desconecta un puerto si este tiene excesivas colisiones.
- Manejabilidad en la RED.

4.4.7 Módulo Modelo 3304 ST FOIRL Host

El módulo 334 ST FOIRL (Fiber Optic Inter-repeater link; enlace inter-repetidor de fibra óptica) , contiene las siguientes características (Ver figura H del apéndice):

* Seis puertos para conexiones con cable de fibra óptica a transmisor/receptor o tarjetas de interfase de red.
* Dos conectores de fibra tipo ST por puerto
* Por puerto , bajo nivel de detección de su función (estado del enlace)
* Autoparticionamiento por puerto, el cual desconecta un puerto si existe excesivas colisiones
* Manejabilidad en la Red
* Soporte para 50/125 um, 62.5/125 um y 100/140 um de fibras ópticas

El puerto RX (recibe) del equipo remoto, es conectado al puerto TX (transmite) del módulo huésped, y el puerto TX del equipo remoto es conectado al puerto RX del módulo huésped.

Los indicadores de este módulo son :

Module LEDs	Status	verde	Modulo esta recibiendo energía
	uP Fault	ámbar	Un falla en el microprocesador ha ocurrido en el tablero. También este led se encuentra encendido mientras se realiza una autoprueba o se haya dado un reset
Port LEDs (4 sets)	Active	verde	Este LED esta encendido cuando el puerto esta operando y conectado a un nodo que se encuentra activo.
	LEM	ámbar	Este LED esta encendido cuando el monitor de error de enlace (LEM) ha detectado que un puerto ha excedido el porcentaje de error a través del NMM
	Fault	ámbar	Este LED se encuentra encendido cuando por un error ha sido aislado el puerto.

4.4.8 Módulo Modelo 3305 UTP Host

Este contiene las siguientes características (Ver figura I del apéndice):

* 12 puertos para conexiones UTP a transmisor/receptor LattisNet o tarjetas de interfase de red

- Conectores hembras RJ-45
- Función del status por puerto
- Autoparticionamiento por puerto
- Red manejable

4.4.9 Módulo Modelo 3368 LattisSecure Host

Este módulo ofrece un nivel básico de seguridad en red. Ver figura J del apéndice. Este protege la privacía de los datos una vez que esta en la línea de dos formas:

- Te previene de usuarios no autorizados, observando el monitoreo de trafico de la red permite limitar deliberadamente de que en un paquete Ethernet pase solamente por el puerto que ha sido autorizado coincidiendo la dirección MAC.
- Otro es a través de conexiones de hardware a la red. El control de intrusos trabaja comparando la dirección MAC fuente que ingreso con el paquete recibido a la dirección autorizada del puerto del módulo 3368. Si la dirección no coincide, el puerto puede ser segmentado por el backplane del controlador.

4.4.10 Módulo Modelo 3333 y 3334-ST Retiming

El controlador 3000 requiere un módulo que realice la función del repetidor que requiere IEEE802.3 para cada segmento Ethernet. La función del repetidor puede ser realizado por un módulo " retiming" o un módulo administrador de red. Ver figura K del apéndice. Esta función lo realizan los módulos 3333 y 3334-ST.

El modelo 333 requiere un puerto AUI para conexión a otros controladores o equipo de red. El módulo 3334-st requiere un puerto de fibra óptica.

4.5 SOFTWARE DE ADMINISTRACIÓN DE RED

El software de administración de red, llamado "agentes" , instalado en los módulos de administración de red (NMMs) tiene la capacidad de recabar información acerca del dispositivo y responde a instrucciones de control específicas. Este tipo de agentes son básico y avanzado.

Un agente básico en un dispositivo Ethernet tiene las siguientes características:

- Pantalla expandida de la red -describe el controlador de la parte de enfrente con la actividad de los LED's residentes de la NMM, módulos huéspedes y módulos interconectados.
- Estado de la información del controlador, ranuras y puertos.
- Información del desempeño a cerca de los marcos de información, bytes, errores CRC (Cyclic Redundacy Check), errores de alineación y colisiones

Un agente avanzado tiene las siguientes características:

- La autopología puede descubrir y mantener una topología lógica y física de: puentes y controladores. Se visualiza esto en un mapa de tiempo real de la red
- Muestra los nodos
- Administrador de ancho de banda
- Seguridad en nodos -permite la creación de una lista arriba de 800 direcciones MAC autorizadas. Este agente automáticamente niega el acceso a usuarios no autorizados y notifica al administrador de la red.
- Colocación de un umbral- 48 umbrales (número de ocurrencias) para el modelo 331xA y 288 para el modelo 331xS pueden ser colocados como medida y deja rastros de eventos en red, incluyendo porcentaje de errores de datos, fallas de apagado y eventos cortos que identifican problemas tales como fallas de NICs (Netware Interface

Card), errores de cableado o problemas de interferencia electromagnéticas. Si un umbral es excedido, los administradores de red pueden determinar la respuesta, tales como un particionamiento automático, segmentación o alarma, y todos los eventos son registrados en una base de datos residente para auditar más tarde.

Vista Expandida	si	si
Puertos habilitados/desabilitados	si	si
Estadísticas de diagnóstico	si	si
Estadísticas de desempeño	si	si
Lista de nodos permitidos	no	si
Umbrales	no	si
Administrador fuera de banda	no	si
Topología automática	no	si

4.5.1 Módulos administradores de red Modelo 331xA y 331xS

Todos los módulos lattisnet administradores de red del sistema 3000 incluyen el protocolo Internet (IP) requerido para soportar el agente controlador de la red básica LattisNet y otros sistemas administradores compatible SNMP. Ver figura L del apéndice. Las versiones también disponibles que incluyen una licencia para soportar un agente administrador de red avanzado y controlador Lattisnet para aplicaciones UNIX.

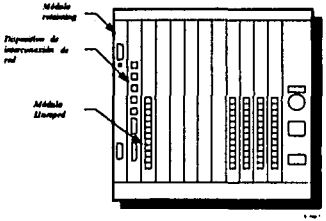
Cada módulo también contiene un puerto RS-232 para tener cavidad a un modem externo para soportar capacidades de señalamiento de fuera de banda.

Específicamente, el 331xS tiene la arquitectura de un procesador dual para una alta rapidez de análisis, soportando un volumen alto de distribución, tipos de protocolo y trafico de fuente/dirección, y 228 umbrales más.

El modelo 3313A y el modelo 3314A NMM contiene virtualmente toda la capacidad de administración del el modelo 3313/14S NMM con la capacidad de soportar el canal A o B. Un jumper sobre el módulo selecciona cual canal del módulo accesar. Esos módulos pueden manejar el *canal a* o el *canal b* pero no ambos al mismo tiempo. Esos módulos NMMs están disponibles dentro de todas las variaciones estandars de los módulos administradores de red Ethernet Lattisnet Synoptics, incluyendo una selección de agente básico o avanzado y AUI o puertos interconectados de fibra 10BASE-FL.

Ambos modelos NMMs 331xA y 331xS contienen cargado localmente opciones para actualizar el software. Sin embargo, el código de imagen en el modelo 331xA esta almacenado en la flash EEPROM (Electrical Erasable, Programable, Read-Only Memory), permitiendo nuevo código a ser reinstalado sobre la red. Actualizar el software en el modelo 331xS requiere un cambio de EEPROM.

4.8 RECOMENDACIONES AL INSTALAR MODULOS



Cuando hay múltiples segmentos administrados en el controlador, el módulo administrador de red (NMM) por cada segmento debe ser colocado en la ranura más a la izquierda. En el controlador mostrado, hay cuatro segmentos administrados, cada uno con una NMM como se muestra en la figura. Si un segmento no tiene una

NMM, entonces el módulo "retiming" debe ser instalado. El orden para colocar módulos en el controlador es de izquierda a derecha y como sigue:

* Modulo "retiming" o NMM
* Módulos de interconectividad
* Módulos huésped o "host"

Si ambos canales A y B son usados y sus administradores de segmentos, el canal A tiene prioridad en el ranura 1. Otros ranuras no tienen prioridad particular. Solamente el modelo 331xA NMMs pueden accesar al canal B. Versiones anteriores de NMMs podrían ser usadas en el segmento del canal A.

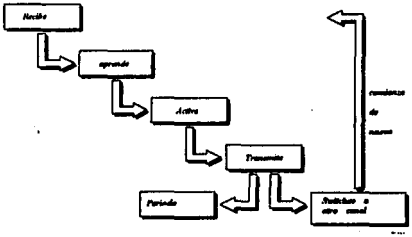
4.7 PUENTES ETHERNET

El puente Ethernet funciona en la subcapa MAC de la capa de enlace de datos. Un puente MAC son dispositivos de "almacena y transmite". En un puente con dos puertos, esto significa que un puente recibe un marco de información completo, entonces decide transmitir este a la red conectada a este otro puerto.

Un puente lee la dirección fuente de cada servidor de la red y construye una tabla que guarda las direcciones en cada lado de el puente. Cuando un marco de información es recibido por el puente, este compara la dirección destino a este siguiente la tabla (este proceso es llamado "filtración"). Si el destino esta en el mismo lado del puente , el puente no transmite el marco de información. Si el destino no esta en el mismo lado como el transmisor, el puente transmite el marco de información. Si el puente no sabe donde enviar el paquete, este emite a todos los puertos excepto del cual se recibió el marco de información (este proceso es llamado desbordamiento).

La familia de productos 3000 incluye módulos de puente Ethernet opcionales. Los puentes pueden unir dos o más segmentos dentro de una simple red lógica. También sirve para dividir una red grande en pequeños segmentos, reduciendo trafico en la red. La principal ventaja de este puente es la habilidad de aislar trafico local del tráfico de otros segmentos de red. Este reduce trafico en la red: si el trafico es lento en la comunicación en red, el problema puede ser resuelto dividiendo la red en segmentos conectados por uno o más puentes. Un puente de red, si bien es dividido en múltiples segmentos, este parecerá como una simple red a los usuarios, mientras la eficiencia y respuesta de tiempo mejorará.

4.7.1 Procesos del puente



El proceso del puente incluye lo siguiente:

* Recibir procesos: un puente de dos puertos recibe trafico de red en ambos puertos, y almacena todos los marcos de información recibidos dentro de la memoria de almacenamiento temporal del servidor.

* Proceso " learning"(estudio) : el puente busca el campo de la dirección fuente MAC de cada servidor que este recibiendo, y agrega una entrada a este a la tabla de transmisión cuando encuentra una dirección desconocida. Cada tabla de transmisión contiene información indicando cuando una dirección fuente esta dada en el lado del puente.

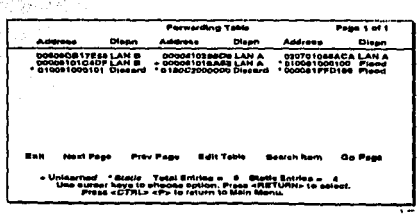
• Proceso de activación: si el camino del destino del marco de información pasa a través del puente, un puente que esta dentro del estado de transmisión despachará el marco de información. Si una entrada de la tabla de transmisión esta en el mismo segmento de red en el momento de envío a la estación, el puente descarta el marco de información. Normalmente, si el puente no encuentra su equivalente en la tabla, este transmite al servidor.

• Proceso de transmisión: el criterio de transmisión puede ser determinado automáticamente por el proceso de estudio o configurado a través de la capacidades de administración del puente. Cuando esta listo para la transmisión, el marco de información es sometido al proceso de transmisión. Este proceso envía el marco de información fuera de la red, si el medio físico es disponible para transmisión. Si el transmisor esta desabilitado, o muchos marcos de información se quedan en espera para transmitir, el puente descarta el marco de información

• Control de selección a otro canal: el control de selección del puente a otro canal recibe el siguiente marco de información.

• Proceso de envejecimiento "aging".- cada entrada que ha sido dinámicamente agregada a la tabla de transmisión tiene un campo "aging". Este campo es inicializado en el tiempo que la dirección de entrada es hecha. Este es reinicializado sobre el receptor del puente de un servidor con una dirección que concuerde, y la entrada es marcada como activa. El campo es decrementado, entonces marca inactivo dos minutos después que la transmisión de la estación fuente ha cesado. Después la entrada ha sido inactiva por más de 24 horas, la entrada es borrada de la tabla de transmisión.

4.7.2 Tabla de transmisión



Un puente local del sistema 3000 contiene una tabla para averiguar e/o introducir direcciones fuentes en estaciones sobre las redes conectadas. Esta es conocida como la tabla de transmisión. Una tabla de transmisión para un puente local puede contener un número máximo de 8192 entradas, incluyendo tres entradas reservadas.

Cada entrada que el puente agregue como el resultado del proceso de estudio es una entrada dinámica. Cuando una entrada es insertada por primera vez en la tabla, esta activa y puede ser usada para determinar si o no envía el frame. El proceso de envejecimiento borrará una entrada dinámica que haya estado inactiva por 24 horas.

Una entrada agregada a la tabla de transmisión del administrador del puente es llamada entrada estática. Una entrada estática se mantiene en la tabla de transmisión hasta que es borrada por otra acción del administrador del puente o por un reset al puente. El proceso de envejecimiento no puede borrar una entrada estática. Los campos de la tabla de transmisión son :

* Address.- la dirección MAC de una estación

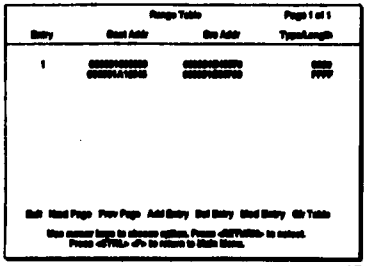
* Dispositon.- ya sea o no los marcos de transmisión del puente las cuales las direcciones destino deben coincidir con las direcciones de entrada. Valores incluidos:

- Transmisión al puerto A
- Transmisión al puerto B
- Desborde
- Descartar (si recibió sobre otro canal)

* Type- estática o dinámica; en los puentes lattisnet SynOptics, una entrada estática es identificada por el símbolo de suma (+) adelante de esta.

* Status- activo o inactivo; en el puente lattisnet SynOptics, un estado olvidado es identificada por un asterisco (*) en frente de este.

4.7.3 Mecanismo de filtración

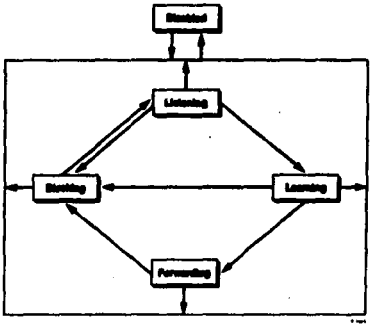


En la operación normal, un puente descarta un marco de información si el destino y el fuente están en el mismo segmento de red. Esta operación de transmisión solamente los marcos de información que conocen un criterio dado o serie de criterios es llamado filtración. En resumen a este básico procedimiento de filtración, un puente local lattisnet SynOptics usa dos mecanismos de filtración:

* Filtración dirección/arreglo: el campo de arreglo de una entrada puede ser puesta con una entrada estática. El filtrado es basado en la dirección destino, el cual es comparado con la entrada estática.

* Filtración de rango: basado en la tabla de direcciones y tipos de paquetes.

4.7.4 Estados de los puertos en puentes



El estado de cada puerto determina si un puerto es parte de la actividad en la topología, y como un marco de información envía a un puerto a ser procesado.

* Blocking/Standby (Bloqueando/en espera): el puerto no participa en el proceso del marco de información, así previene duplicaciones procediendo a través de múltiples vías en la topología. Marcos de informaciónes recibidos son descartados, la información de la estación no es agregada a la base de datos del filtrado.

* Listening (escuchando): el puerto esta preparando participar en le proceso del frame, pero este es temporalmente desabilitado para prevenir loops temporales. Los marcos de información son descartados, la información de la estación no es incorporada en la base de datos del filtrado.

* Learning (aprendiendo): el puerto esta preparando participar en le proceso del frame, pero este es temporalmente desabilitado para prevenir loops temporales. Los marcos de información son descartados, la información de la estación es incorporada en la base de datos del filtrado.

• Forwarding (transmitiendo) : el puerto esta participando en el proceso del frame, el puerto de transmisión recibe marcos de información y admite marcos de información transmitidos para transmisión. La información de la estación es incorporada a la base de datos del filtrado.

• Disable (desabilitado) : el puerto no esta participando en ninguna actividad

4.7.5 Protocolo de árbol expandido (Spanning Tree Protocol)

En una configuración redundante, más de un puente puede ser instalado entre segmentos de red. Una configuración redundante tiene la ventaja de tener una tolerancia de falla. Cuando un enlace falla, el tráfico puede ser automáticamente transmitido a través de otra vía.

Potencialmente, si los paquetes destinados por otro segmento son misteriosamente transmitidos por más de un puente, múltiples respuestas se pueden generar, cada una de las cuales, en su turno, pueden generar múltiples respuestas. Un crecimiento exponencial en el número de paquetes que ocurren, rápidamente inundan la red. Previniendo esta situación se requiere el uso de un software del puente que mantenga solamente una vía activa entre los segmentos de red. El protocolo de árbol expandido (spaning tree protocol) contiene esta capacidad.

En resumen, el protocolo de árbol expandido contiene una tolerancia de falla a través de la reconfiguración automática del puente en el caso de una parada imprevista en la ruta de datos. La eliminación de loops y la reconfiguración automática son transparentes para los nodos, los cuales transmiten datos por el mismo camino, sin hacer caso de que vía esta activa.

Cuando en un puente se conectan dos redes, una única vía existe entre las dos redes. Cuando en un puente se conecta múltiples redes, más de una vía puede existir de una red a la siguiente.

4.7.6. Módulos Puente Modelo 3323S y 3324S-ST

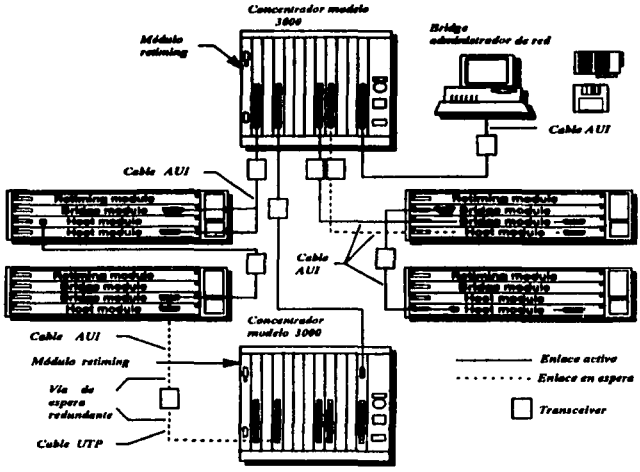
El modelo 3323S y el modelo 3324S-ST High-Speed Local Ethernet Puentes interconectan segmentos Ethernet a una forma simple, transparente para la red. Ver figura M del apéndice. Estos sirven también para dividir una red grande en dominios de colisiones locales pequeños, reduciendo trafico en la red. En resumen, los puentes pueden tener sustituciones de enlaces en controladores que pueden ser activados automáticamente si el enlace primario falla. Estos puentes locales Ethernet soportan dos tipos de STP - Draf t 8 (basado por redes pre-802.3) y rev. C del estándar IEEE 802.1 La rev. C es el dafault tipo STP soportado. El estandar IEEE 802.1 define las especificaciones para puentes, incluyendo el protocolo de árbol expandido.

El puente contiene una capa en el bus de datos Ethernet sobre el backplane de los controladores Ethernet y son operacionales sin adicionar configuración. Estos filtran el trafico de la red y transmite los datos del marco de información destinados a otros segmentos de la red. El software administrador del puente local contiene funciones de monitor y control de una consola central de monitoreo y en el cual se visualiza datos estadísticos de los datos recibidos de los puentes.

Los puentes del sistemas 3000 filtran trafico en la red hasta por 29,000 marcos de información por segundo cuando el filtrado y la transmisión 13,650 datos de los marcos de información por segundo cuando transmite bidireccionalmente:

* El modelo 3323S contiene conexión para UTP, cable coaxial o fibra óptica a través de un puerto AUI.
* El modelo 3324S-ST tiene como característica la conexión de una fibra óptica dúplex interrepetidor enlace (FOIRL) puerto con tipo ST conectores bayoneta para conectar los backbones de la fibra óptica y soportar distancias arriba de dos kilómetros entre controladores.

4.7.7 Pauta para configurar un puente local



La figura muestra la configuración de una red con módulos de puentes locales Ethernet. Los controladores con los puentes locales requieren un módulo "retiming" Ethernet o un módulo administrador de red Ethernet para dar la función "retiming".

Obsérvese la norma general del siguiente configuración del puente:

Diseñar la red como si el puente no estuviese presente. Entonces configurar los puentes conveniente la topología doseada. Si esta práctica es buena agregar la regla 80/20. Acorde a esta regla, 80 por ciento del tráfico de un segmento debe ser local, y el 20 por ciento puede ser direccionada a otros segmentos.

Un puente puede funcionar sin alguna modificación de estos parámetros. Los parámetros del puente deberían ser modificados solamente para asegurar una topología en particular o para determinar cual enlace redundante será activado durante una falla.

La prueba SQE (Signal Quality Error) no necesita estar desabilitado sobre el transmisor/receptor conectado que es usado con el puente para controladores interconectados.

4.8 MODULO ETHERNET SWITCH ENGINE (ESE)

El módulo "Ethernet Switch Engine" (Mecanismo de conmutación Ethernet "ESE") consiste de tres principales componentes: el módulo del sistema, la matriz de cambio punto-cruzado, el paquete de procesadores Ethernet (EPP's)

* El módulo del sistema es responsable del mantenimiento de las tablas de direcciones en cada módulo ESE y de la comunicación con la estación administradora de red.
* La matriz de cambio punto-cruzado contiene conexiones para EPPs y el módulo del sistema
* Los EPPs desempeñan los cambios, transmiten paquetes al puerto apropiado basados en las direcciones destinos en la cabezerá del paquete y el contenido de una tabla de direcciones por cada uno de los EPPs.

4.8.1 Procesameinto de paquetes

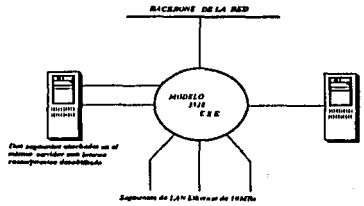
El módulo ESE opera en la capa de enlace de datos, llama todo lo que se encuentre en esta capa. Normalmente, el procesador "lee" el paquete entero, entonces envía este a la capa física. El procesador ESE lee los primeros seis bytes del paquete que viene, el cual contiene la dirección destino. Este entonces, comienza transmitiendo este a través de la conexión dedicada que establece la matriz punto-cruzado. Así, mientras el resto de los paquetes esta siendo leído en un puerto, los primeros seis bytes están iendose fuera del otro puerto. Esta tecnología de cambio apresura el procesamiento del paquetes y minimiza la necesidad para almacenar paquetes.

4.8.2 Módulo Modelo 3328 ESE

Este módulo contiene las siguientes caracetrísticas (Ver apéndice N) :

* 5 conectores RJ-45 en donde se conectan segmentos Ethernet
  - Cuatro conectores RJ-45
  - Un conector configurable de RJ-45 a AUI
* 1 puerto de consola RS-232
* Indicadores de LEDS para configuración de puertos e información de status
* Un inicializador del conmutador

4.8.3 Pauta para configuración



* Utilizado en donde accesan multiples servidores y se genera un excesivo tráfico.

* En redes segmentadas por un módulo ESE, se tiene múltiples vías para accesar servidores.

Con lo anterior, se concluye con la descripción de cada uno de las características de los módulos que componen al controlador lattisnet Series 3000 y la forma de ver el estado de cada módulo físicamente.

CAPITULO 5 PROCEDIMIENTO PARA EL MONITOREO DE UNA RED LOCAL

El monitoreo es la parte esencial del buen funcionamiento de la red, para ello se necesitan de herramientas para realizar este mismo. En este capítulo se describirá el funcionamiento y las características del software de monitoreo Optivity así como la función y configuración de los módulos NMM's.

5.1 ADMINISTRACION DE REDES

La administración de redes es el proceso que se lleva a cabo para controlar una red de datos compleja de forma que se aumente su eficiencia y productividad.

El objetivo de fondo de la administración de redes, más allá de detectar y corregir fallas, es proporcionar a la red una herramienta de trabajo confiable para las organizaciones. Al tener un sistema confiable, la eficiencia y productividad en forma considerable.

Conforme las redes departamentales de pocos usuarios se interconectan con otras redes departamentales dentro de la organización, ya sea en el mismo edificio o en edificios diferentes, mantener el control y la correcta operación de cada una de esas redes individuales se convierte en una actividad compleja.

La red se vuelve compleja al tener un gran número de usuarios en localizaciones geográficas diferentes y con tecnologías de redes diversas operando entre sí. Los problemas para mantener un sistema así funcionando son de todo tipo, desde fallas en el cableado hasta en aplicaciones especializadas.

La ISO define 5 áreas funcionales de administración de redes y podemos añadir una sexta que se denomina mesa de ayuda o mejor conocida como "Help desk".

5.1.1. Administración de fallas

Es el proceso mediante el que se localizan problemas o fallas en la red de datos. Se componen de 3 elementos:

1. Detectar el problema, en algunos casos antes de que se presenten
2. Aislar el problema
3. Corregir el problema, si es posible.

Con el uso de herramientas de administración de redes se pueden localizar y corregir problemas de manera más rápida. Para detectar el problema debe estar definidos los elementos de los que se va obtener información de la red y establecer niveles y prioridades para cada uno de ellos. No hacer esto puede provocar:

a) Recibir una avalancha de mensajes de fallas no importantes

b) Recibir las alarmas verdaderamente críticas con una prioridad mal definida

Una vez detectado el problema debe ser capaz de detectar la existencia de un problema y dar los mecanismos necesarios para aislar el problema.

Una vez determinado el problema, la herramienta debe preferentemente ser capaz de corregirlo. Normalmente se utilizan códigos de colores para detectar, aislar y corregir el problema.

5.1.2 Administración del rendimiento

Consiste en garantizar que la red se mantendrá siempre accesible con tiempos de respuesta aceptables de manera que los usuarios puedan utilizarla en forma eficiente.

Permite también el crecimiento de la red y su impacto en el rendimiento futuro. Esto se lleva a cabo mediante el monitoreo constante y la corrección de los problemas de rendimiento que presenta la red.

Para llevar a cabo el monitoreo del rendimiento se deben seguir los siguientes pasos:

1. Obtener los datos de la utilización de dispositivos de la red o sus enlaces.
2. Analizar datos relevantes para detectar puntos de alta utilización.
3. Establecer umbrales de utilización tolerados.
4. Hacer un modelo manual o automático para proponer modificaciones que aumenten el rendimiento

Este mismo esquema puede ser utilizado no solamente para detectar los puntos en donde el rendimiento actual es bajo; sino que permite planear el crecimiento futuro de la red en base a las tendencias en la utilización.

5.1.3 Administración de la configuración

Consiste en obtener datos en línea de la red para mantener el control de todos sus dispositivos. Para llevar a cabo la administración de la configuración es necesario contar con herramientas capaces de detectar y obtener información sobre los dispositivos de la red y guardarlos en una base de datos para su uso posterior.

En una red compleja los constantes cambios y modificaciones hacen que pierda fácilmente el control de la configuración de la red y sus dispositivos. Normalmente el inventario que se tiene por escrito difiere de lo que realmente está instalado en la red.

La administración de la configuración puede llevarse a cabo a niveles tan avanzados que permita accesar y controlar tanto las versiones de software y licencias a lo largo de la red, como la distribución automática de software o actualizaciones.

5.1.4 Administración de la seguridad

La administración de la seguridad consiste en proteger la información sensible que se encuentra en los dispositivos de la red al controlar los puntos de acceso a esa información.

La administración de la seguridad involucra los siguientes pasos:

1. Identificar la información que debe ser protegida de acuerdo a las políticas y mecanismos de confidencialidad de la organización. Debe determinarse cual información es pública y cual debe tener restricciones de acceso.

2. Encontrar y asegurar los puntos de acceso. No solamente las computadoras que están conectadas a la red, sino los servidores y comunicaciones remotas, deben tener mecanismos de seguridad establecidos. Existe seguridad a nivel sistema operativo y seguridad a nivel físico.

3. Mantener el sistema de seguridad. El sistema de seguridad debe ser a la vez dinámico y estricto; así como también debe poder detectarse los intentos de violación a la seguridad.

5.1.5 Administración de costos

Las organizaciones están divididas en áreas funcionales y es importante para muchas tener identificados los costos reales por departamento o división.

La administración de costos permite prorratear los costos totales de la función informática de la organización por centro de costos, obteniendo así información real de el uso de los recursos de red de cada uno de los usuarios, departamentos o divisiones.

5.1.6 Mesa de Ayuda

El servicio, soporte, reporte de problemas, seguimiento de problemas y estadísticas de fallas de una red compleja se vuelven actividades en las que se puede perder fácilmente el control. Un sistema de mesa de ayuda permite automatizar los procesos mencionados, aumentando el nivel de servicio que se le da a los usuarios de la red.

5.2 OPTIVITY Y LA ADMINISTRACION DE AMBIENTE EN RED

Optivity es una serie de programas de aplicaciones de administración en red. El software de administración de red de Optivity proporciona herramientas para el manejo de las LAN's , mientras se observa como cada LAN esta integrada dentro del ambiente de red. Optivity esta disponible para las siguientes plataformas de administración de redes:

- HP Open View/Dos
- Novell Netware Management System
- SunNet Manager
- HP Open View/UNIX
- IBM NetView/6000

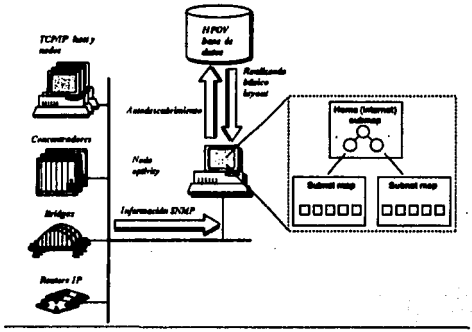
5.2.1 Administrador SNMP

SNMP ("Simple Network manager Protocol" ; Protocolo Simple de manejo de redes) define el mecanismo de transporte que los agentes, los cuales recolectan información que usan para el intercambio de información con otros administradores SNMP. La información recolectada es organizada en una base de datos llamada MIB ("Management Information Base" ; Base de Manejo de Información).

5.2.2 Características del HP OpenView

OpenView contiene un número de características básicas que son usadas por Optivity y otras aplicaciones Open View, incluyendo las siguientes:

* *Static maps (mapas estáticos)*



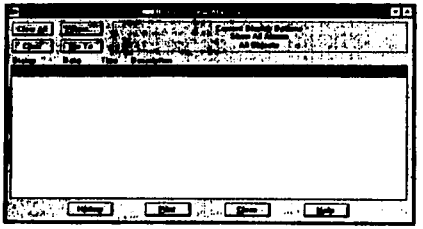
"Open View" tiene la característica de autodescubrir información que contiene todo acerca de los dispositivos SNMP en una interred y almacena esto en una base de datos. Se usa la opción básica de layout para generar los mapas estáticos del "Open View" de esta base de datos. Esta opción genera un archivo que contiene un submapa principal "home submap" y un submapa de la subred por cada IP de subrred descubierta.

El submapa principal contiene un símbolo por cada ruteador y por cada subred. Dando un doble click sobre el símbolo de la subred, se pueden abrir dispositivos submapas por cada subred. El dispositivo submapa es

llamada por la dirección IP y contiene un símbolo para cada dispositivo IP descubierto a través de autodescubrimiento "Open View".

Los mapas de Open View son llamados estáticos porque no se actualizan automáticamente cuando los cambios ocurren en la red. Los cambios son automáticamente colectados por el autodescubrimiento y almacenados en la base de datos de acuerdo a la lista configurable. Sin embargo, se debe usar la opción del layout básico para regenerar los mapas que reflejen la nueva información.

* *manejador de alarmas*



Este es utilizado para visualizar los mensajes de alarma actuales. Para visualizar hay que seleccionar "monitor" y después "Alarm Log". De la ventana principal de "Open View" se despliega la ventana de "Alarm Log". Los mensajes de alarma son salvados en " Alarm Log".

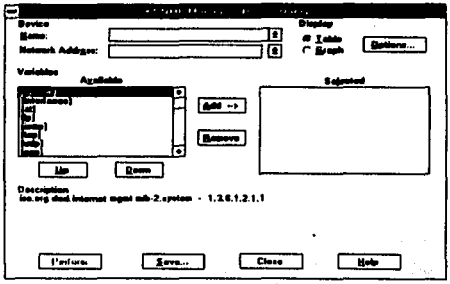
El control de los tipos de alarmas y las clases de dispositivos para los cuales las alarmas son vistas, hay que usar el botón sobre la ventana de "Alarm Log". Se visualizara un mapa conteniendo el dispositivo afectado seleccionando un mensaje de alarma y dando un click en el botón "Go to"(ir a).

Las alarmas son generadas por efectos SNMP o por condiciones excesivos de umbrales en Optivity. Cuando una alarma ha sido generada por un dispositivo, el símbolo de Open View para el dispositivo afectado cambia de color. El color de los símbolos de la subred sobre el submapa principal indica la más alta severidad de alarma recibida por algún dispositivo dentro de la subred.

La siguiente tabla muestra las diferencia entre colores y niveles de gravedad

Crítico	Rojo	Normal	Verde
Mayor	Rojo oscuro	Desconocida	Azul
Menor	Naranja	Desabilitada	Cian
Advertencia	Amarillo	Información	Morado
Margen	Amarillo-verde	Inmanegable	Blanco

* *administrador SNMP*



El administrador SNMP contiene las siguientes tres opciones:

1) Define consultas.- permite identificar el tipo de información a obtener del dispositivo SNMP e

identifica la dirección de red del dispositivo.

2) Selecciona consultas.- permite seleccionar una consulta definida previa

3) Manejo de base de datos.- permite seleccionar archivos de la base de datos del MIB para ser compilada.

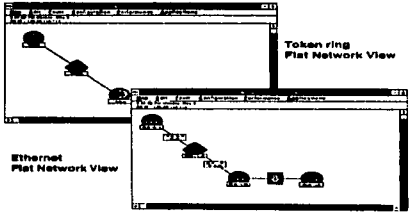
5.2.3 Características y opciones de Optivity

Optivity contiene caracteristicas que forman y mejorar la funcionalidad dada por "Hp Open View". Mientras "Open View" te ayuda a entender la topologia de la red e identificar problemas que ocurren, Optivity contiene más pantallas detalladas y auxilia en eventos aislados. Optivity contiene información especifica y da un control a nivel de puerto sobre los concentradores Lattisnet SynOptics y dispositivos conectados.

La autotopologia Optivity complementa al autodescubrimiento de "Open View", da información requerida para crear pantallas dinámicas. En Optivity son llamadas pantallass dinámicas porque pueden ser actualizadas y reflejan cambios en la red. Actualizar una vista Optivity, se usa la opción "Validate" (validar). Las siguientes pantallas son disponibles del menú "Open View Aplications":

* *Pantalla del plano de la red (Flat Network View)*

En este punto se observa como los segmentos de red son conectados por puentes o conmutadores.



La pantalla del plano de la red muestra símbolos de segmentos Ethernet o Token Ring conectados por símbolos de puentes. Optivity contiene una pantalla del plano de red para cada subred IP, enlazada al símbolo de subredes sobre el mapa principal de "Open View". Para ver una pantalla del plano de la red, seleccionar el símbolo de la subred sobre el mapa principal, y seleccionar "Flat Network View" de menú "Open View Applications".

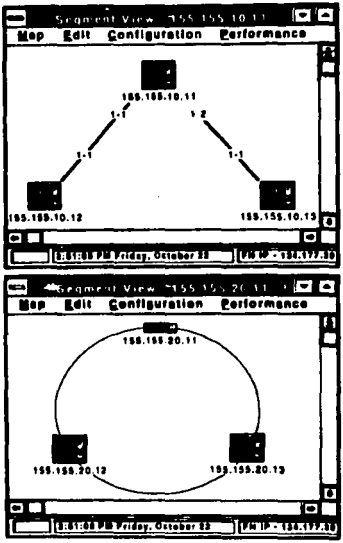
Porque son dinámicas, se puede usar las pantallas de planos de la red para observar la topología actual Ethernet o Token Ring y monitorear los cambios, También provee un concisa pintura de la capa de enlace de datos relacionada a los segmentos entre redes.

Las pantallas de los planos de la red despliega segmentos que contienen un modulo administrador de red SynOptics (NMM) con un agente SNMP avanzado. Cada símbolo de segmento es identificado por la dirección IP de esta NMM. Bridges o segmentos que dejan de estar disponibles son vistos en rojo en el "Flat Network View". Para borrar permanentemente estos símbolos del mapa, seleccionar "Remove Red OPtion" del menú "Flat Network Edit".

El "Flat network view " contiene la opción de desplegar información acerca de la dirección IP de la NMM el cual el puente es conectado y el slot del concentrador y número del puerto de la conexión.

* *Pantalla del segmento (SSegment View)*

De la pantalla del segmento se pueden realizar el monitoreo de red y operaciones de administración sobre controladores Lattisnet synOptics dentro del dominios de colisiones Ethernet o Token ring.



Para visualizar la pantalla del segmento por cada segmento, dar un click en el símbolo del segmento sobre un "Flat Network View" o un mapa subred de "Open View" y seleccionar la opción "Segment View" del menú "Open View Applications".

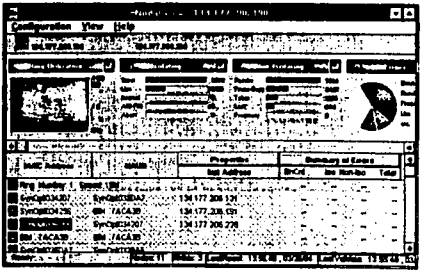
La pantalla del segmento permite realizar administración de red a nivel del concentrador para concentradores en agentes avanzados. La pantalla del segmento despliega símbolos que indican el tipo de concentrador y estado, y da la dirección IP de agente SNMP avanzado sobre cada concentrador.

Una típica pantalla del segmento para segmentos Ethernet o Token Ring muestran la siguiente información:

- Símbolo del concentrador sobre el segmento de red
- Dirección IP del el agente SNMP en cada concentrador SynOptic sobre el segmento
- Indicadores en color mostrando el estado de cada controlador
- Líneas que muestran las conexiones entre controladores
- Notificaciones enviadas por los agentes SNMP corriendo sobre los controladores SynOptics
- Barra de menú que incluye mapa y menús de configuraciones
- Menú por cada símbolo SynOptics, mostrando acceso a estadísticas de ventanas y Expanden View.

La pantalla del segmento para Ethernet también identifica los puertos a través de los cuales dos controladores están conectados. Esta es una particular uso cuando se haya de realizar la documentación de la topología física de la red o cuando eventos aislados de red en el concentrador hayan ocurridos o nivel de concentrador.

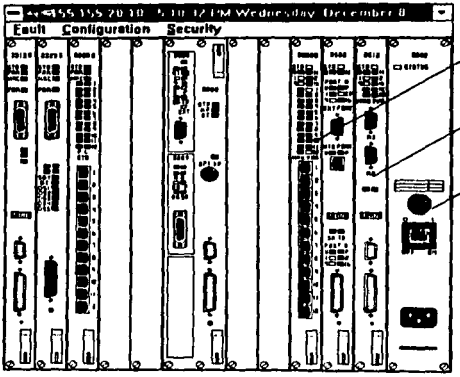
* *Pantalla de nodos ("Nodal View")*



"Nodal View" (pantalla a nivel de nodo) proporciona información acerca de los nodos IP conectados a los dispositivos manejables SynOptics. Se usa ésta pantalla después de haber aislado un evento de red de una LAN específica, aislar el problema de un concentrador, módulo o puerto. Esta pantalla contiene opciones de administración en los segmentos puenteados, controladores, módulos y a nivel de puertos, incluyendo las siguientes características:

- Diagnósticos
- Utilización y otras estadísticas de desempeño
- Servidores y distribución de protocolos (con NMM 331xS solamente)
- Nombres de nodos, MAC y direcciones de red con asociación de puertos
- Sort nodes para diferentes valores
- Menú que dan fault, configuración y opciones de desempeño.

• *Pantalla expandida ("Expanded View")*



La pantalla expandida (Expanded view) muestra detalladamente información acerca de los controladores lattisnet SynOptics y dispositivos conectados sobre redes Ethernet o Token ring. Esta vista esta disponible para cualquier concentrador IP sobre un mapa subred "Open View", incluyendo controladores con agentes básicos. Cuando un controlador contiene múltiples NMMs, una pantalla expandida separada esta disponible para cada NMM. El controlador es igual por cada pantalla, excepto que cada LED o módulos administradores por el NMM seleccionado esta en verde.

Cada pantalla de Optivity contiene opciones para fallas, desempeño, configuración y administración de seguridad. Las siguientes aplicaciones Optivity son disponibles del menú de aplicaciones de "Open View":

* *MeterMan*

Despliega estadísticas para controladores lattisnet synOptics y dispositivos interconexión de redes dentro de una forma de indicador multicolores. También soporta ciertos dispositivos de interconexión de redes, incluyendo routers Cisco, puentes remotos Retix y terminales de servidores Xyplex.

* *BridgeMan*

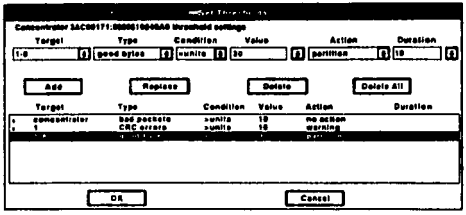
Es una aplicación que contiene la configuración, defectos y pociones de desempeño para puentes transparente y fuentes

Las siguientes opciones Optivity son disponibles del menú de herramientas de "Open View":

1) Estando conectado permite capturar diagnosticas e información de actividad acerca del segmento Ethernet o Token Ring

2) Encontrar nodos permite rápidamente encontrar alguna estación administrable.

* *Thresholds* (umbrales)

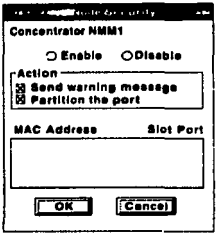


Cada pantalla de Optivity permite obtener defectos, desempeño y menús de configuración que proveen opciones para realizar en diferentes funciones del administrador de red. La opción de umbrales "Thresholds" permite definir un umbral para un evento de red específico, tal como paquetes buenos o Errores FCS. Si el límite definido para un evento esta excedido, el agente SNMP del concentrador envía un umbral excedido al NMS.

Se puede colocar un error, actividad o status de umbrales en el concentrador, tarjeta o a nivel de puerto para redes Ethernet. Para redes Token Ring, se pueden colocar en el concentrador a nivel de anillo.

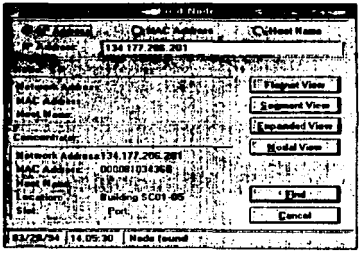
Los umbrales permiten administrar sin tener que monitorear constantemente la red.

• *Seguridad de nodo*



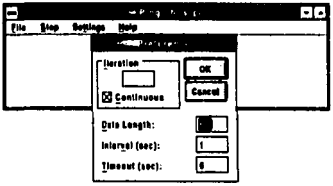
Este permite definir una lista de nodos los cuales se les permitió transmitir más tráfico sobre un controlador en particular, módulo o puerto. Si un nodo no esta en la lista, este es borrado de la red.

• *Encontrar nodo*



Permite un fácil acceso a todas las vista de Optivity para concentradores con agentes SNMP avanzados y obtener de esto es alarmas reportando un problema con un nodo en particular.

• *Ping, telnet y Newt*



Optivity contiene las siguientes tres aplicaciones stándar de TCP/IP que proporcionar cierta información al usuario en la administración de la red:

1) Ping .- esta herramienta puede ayudar en una prueba física, enlace de datos y conectividad en red entre la estación de administración y un dispositivo de la red.

2) Telnet.- permite establecer dos conexiones con un dispositivo remoto sobre interconexion TCP/IP. Esta conexión permite configurar o administrar el dispositivo de la misma manera como si estuviera directamente el dispositivo con una terminal.

3) Newt (NetManage Enhanced Windows TCP/IP).- permite manejar las comunicaciones de estaciones. Se puede visualizar la configuración e información estadística de la interfase de red para nuestra estación administradora.

5.3 PLANEACION DE LA RED

La siguiente lista es una serie de pasos a seguir para preparar la instalación de una red que implica el monitoreo con el administrador de red Optivity. Algunos de estos pasos no serán necesarios para una red que ya este instalada:

1. Manejo del local
2. Mapa de la red
3. Identificar secciones criticas o dominios
4. Identificar interconexiones
5. Crear una lista de equipo por numero de modelo: Sistema 3000, sistema 2000, sistema 500.
6. Localizar puentes, rutedaores y compuertas lógicas de la red
7. Localizar enlaces remotos que se quieran manejar
8. Mapas en papel, direcciones IP, subredes para todos los NMMs, estaciones administradoras de red, y otros dispositivos basados en IP de la red.
9. Instalar software y elementos de hardware.

5.4 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

* *Hardware*

El software de Optivity corre sobre PC-DOS o sistemas operativos MS_DOS (versión 5.x), en procesadores 386 o 484 plataformas 100% compatibles, o IBM PS/2 386. Los requerimientos incluyen el siguiente hardware

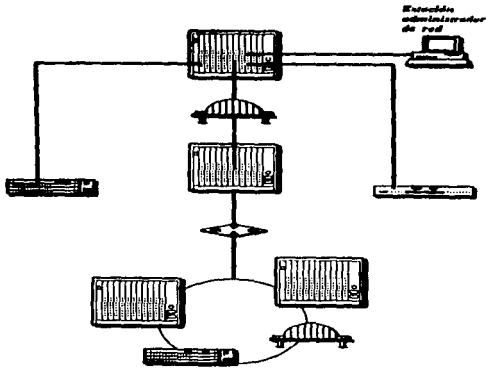
- Estaciones de trabajo 386/486 a 33 MHZ
- 12 MB de RAM (recomendado 16 MB)

- 40 MB de espacio en disco duro
- Monitor VGA
- Mouse
- Tarjeta de red
- Impresora

* *Software*

- Dos 5.0 o versión nueva (6.2 recomendado)
- Microsoft Windows 3.0 o posteriores
- Disquetes Optivity

5.5 COMPONENTES DE UN ADMINISTRADOR DE RED LATTISNET SYNOPTICS



* *Requerimientos NMM*

Se necesita una NMM por cada segmento Ethernet o concentrador Token Ring o anillo físico que se quiera manejar. Si un chasis 3000 contiene ambos módulos (Ethernet y Token ring) este contiene por lo menos dos redes independientes de un administrador. Cada NMM será representada en una pantalla dinámica de segmento como un controlador. Una simple estación administradora de red con tarjetas de interface Ethernet y token Ring puede manejar a ambos. Sin embargo, el orden para pasar tráfico entre las redes Ethernet y Token Ring, estos deben ser conectados a través de un router o un puente traslacional Ethernet-to-Token ring.

* *Puentes y ruteadores*

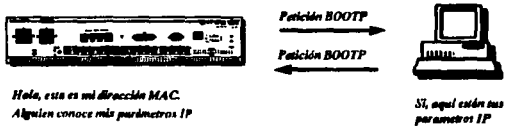
Por que interconectar dispositivos de red tales como puentes y ruteadores, por que son esenciales componentes de muchas redes, la aplicación administradora SNMP permite a la estación de Optivity manejar algún agente SNMP complicado.

5.6 TIPOS DE BOOTS

5.6.1 Booting: BootP

Un dispositivo tal como un puente, conmutador, ruteador, concentrador o NMM, mantiene un programa de arranque en una memoria de sólo lectura (ROM). Este programa tienes dirección de hardware. Cuando este dispositivo arranca, este generalmente obtiene la dirección IP de la información de arranque que reside en algún disco duro o en una EEPROM. La dirección IP es esencial para habilitar la comunicación sobre la red. Las direcciones pueden estar almacenadas en un dispositivo externo al dispositivo, y algunos mecanismos deben determinar como el dispositivo obtiene esta dirección. Uno de estos mecanismos el protocolo bootstrap (BootP).

Cuando un dispositivo intenta un boot usando BootP, este manda un simple mensaje conteniendo su dirección de hardware y requiriendo información necesaria para arrancar tales como su propia dirección IP. El mensaje va a todos los dispositivos, pero solamente el servidor que puede dar la información de arranque responde al requerimiento BootP. El servidor BootP responde con un paquete que incluye la dirección IP del dispositivo; la dirección IP del servidor TFTP que tiene la información de arranque, llama inicialmente la imagen de memoria, para el dispositivo; y el nombre del archivo de configuración del dispositivo almacenado en el servidor TFTP.

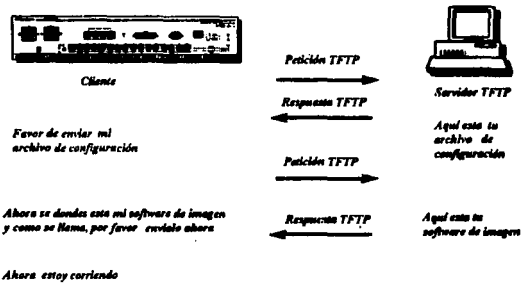


5.6.2 Booting "TFTP".

Después que el servidor BootP responde al requerimiento del cliente BootP, el cliente entonces usa el TFTP ("Trivial File Transfer Protocol"; Protocolo Trivial de Transferencia de archivos) que requiere del servidor TFTP el archivo de configuración identificado por BootP. El BootP y el servidor TFTP son usualmente, pero no necesariamente, el mismo dispositivo.

El archivo de configuración provisto por el cliente por el servidor TFTP especifica el nombre del archivo que contiene la imagen de memoria inicial del cliente, el software de imagen requerido para completar la operación de arranque. El servidor provee al cliente con el archivo conteniendo la imagen del cliente. El cliente almacena esta imagen en memoria de acceso aleatorio (RAM)

La ventaja de usar TFTP sobre las NMMS es que las nuevas versiones de los archivos ".IMG" que almacenan los agentes de dispositivos pueden ser cargados en el servidor TFTP. Esto permite que dispositivos que son inicializados o apagados y regresen a cargar la versión actual de sus imágenes y almacene estas en RAM y flash EPROM, dependiendo del dispositivo. Módulos con flash EPROM solamente necesitan descargare la nueva imagen una vez; después que estos puedan inicializar localmente.



5.6.3 TFTP directo

TFTP directo elimina la necesidad de usar BootP después de la configuración inicial de la NMM. En vez de usar BootP, un dispositivo que usa TFTP direccionado boot usando información almacenada localmente. Esta información incluye su propia dirección IP, el nombre de este servidor TFTP, y el camino completo y el nombre de este archivo ".cfg". Usando esta información, el dispositivo usa TFTP para completar esta configuración y descargar la imagen.

TFTP direccionado es usualmente para inicializar un dispositivo a través de un ruteador no synoptics que no tengan la característica de ayuda IP. porque TFTP direccionado permite especificar la dirección IP del servidor Boot sobre un dispositivo, este no necesita enviar un mensaje BootP que son descartados por los ruteadores.

Para configurar un nuevo dispositivo par usar TFTP directo se deben seguir los siguientes pasos:

1. Manualmente configurar el dispositivo con información boot a través del puerto del servicio o usando BootP
2. Configurar el dispositivo usando EEPROM para información Boot.
3. Escribir la nueva configuración al EEPROM
4. Usar la aplicación BootP/*TFTP* (*BPTFTP*.EXE) para TFTP (para descargar archivos ".CFG" y ".IMG").

5.7 INSTALACION DE OPTIVITY

Antes de instalar Optivity, se debe determinar las direcciones IP y las subredes que existan y que serán usadas en la red. Se deberá de tener un plano detallado de todos los dispositivos que forman la red así como las direcciones IP asignados a estos.

Optivity se almacena en un subdiretorio bajo raíz "C:\optivity". En el subdirectorio Optivity se tiene siete subdirectorios:

1. BIN.- contiene los archivos ejecutables así como otros 3 subdirectorios:
   - LOG.- inicialmente esta vacío, después almacena todos los archivos ".log".
   - SYMBOLS.- almacena los símbolos de Optivity
   - THRESHOL.- almacena errores de datos

2. COMM.- archivos relacionados a la comunicación TCP/IP de la estación Optivity con otros dispositivos de la red.

3. DB.- archivos de la base de datos Optivity

4. IMAGES.- configuración del agente SNMP y archivos de imagen

5. MIBS.- adicionales MIB's SNMP (sin compilar) dado por Optivity

6. OV71.- subdirectorios de HP Open View 7.1 y archivos

- BKGROUND.- background de los mapas para importar mapas a través de "Open View"
- HELP.- archivos de ayuda de "Open View"
- SYMBOLS.- simbolos
- SAVED.- archivos de configuración de estaciones de trabajo respaldados durante la instalación

El programa de instalación deberá poder escribir en los siguientes archivos:

1. C:\windows\progman.ini

2. C:\windows\comm\protocol.ini

3. C:\autoexec.bat

4. C:\config.sys

5. C:\windows\win.ini

Se tiene una aplicación denominada "Custom" (personalizar) , que permite configurar las comunicaciones TCP/IP para el nodo de monitoreo. Durante la instalación de Optivity se deberá completar los datos requeridos en el programa de windows "Custom". Estos datos son: Dirección IP, Subnet Mask (máscara de la subred) , Internet Host Name (Nombre del host del internet), Internet Domain Name (Nombre del dominio del internet) .

Para comenzar la instalación seguir los siguientes pasos:

1.Entrar a windows

2. Ejecutar el administrador de programas

3. Insertar el disco etiquetado " Optivity for HP Open View (DOS)-SETUP Disk 1.

4. Seleccionar "ejecutar" del menu "File".

5. Teclear lo siguiente: a:\setup

6. Replazar diskettes en la unidad cuando pida insertar el siguiente

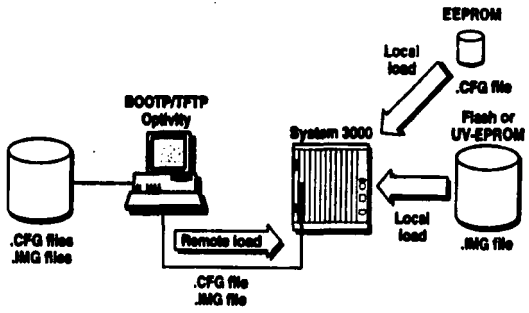
7. Dar un click en OK por cada diskette insertado.

8. Después que son copiados los 12 diskettes, el sistema abre el programa de windows "Custom", en donde se configurará los parámetros de la red para el nodo de monitoreo:

- Seleccionar "Add" del menu "Interface" para agregar una nueva tarjeta de interfase de red.
- Insertar el tipo de enlace para la intefase de la lista que se muestra.
- Seleccionar el tipo de tarjeta del menu "Setup" y seleccionarla.
- Teclear la dirección IP, la subnet Mask, el host name, el default gateway
- Seleccionar el SNMP del menu "Services".
- Todo lo anterior lo salve en c:\comm\tcpip.cfg
- Seleccionar "exit" del menu File.
- Si se nos pregunta reinicializar el equipo, seleccionar "YES"

5.8 EEPROMS Y NMM'S

Todos los NMM's Lattisnet SynOptics tiene información de su configuración y la forma de inicializar dentro de una memoria no volatil llamada EEPROM (Electrical Erasable, Programmable, Read-Only Memory). Esta es un tipo de memoria que puede ser elctronicamente programada y borrada , y no requiere de fuente de poder que retenga los datos.



Los modelos 331xS y 351X almacenan sus imagenes dentro de una EPROM (Erasable, programmable, read-only memory), también llamada UV-EPROM, es borrable solamente con luz ultravioleta, esta no puede ser electrónicamente programable, modificada o borrada por alguna estaci{on de monitoreo que contenga Optivity. De tal forma, que si se desea dar de baja una imagen de alguna de los NMM, la imagen es almacenada en RAM. Cuando se inicializa al módulo NMM o es apagado, la información en la Ram se pierde. Asi que el módulo NMM usa la imagen almacenada en una EPROM. Los modelos 331xSA, 271x y 281x almacenan sus imagenes en una flash EEROM.

5.8.1 BOOTPTAB/TXT

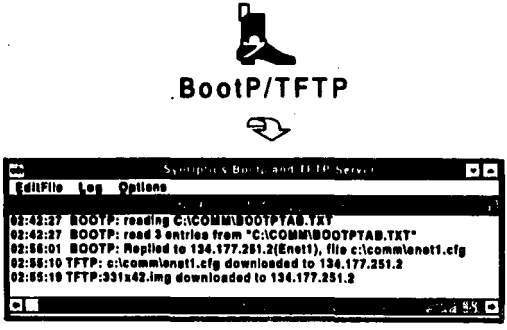
Cada NMM que será reinicializada debe de tener en la estación de monitoreo de Optivity un archivo de entrada llamado " BOOTPTAB.TXT" , el cual contiene toda la configuración y las rutas de las imagenes que conforman a la red. incluyendo direcciones IP. El programa Optivity utiliza como entrada BootP/TFTP

Para accesar al archivo BOOTPTAB.TXT seguir los siguientes pasos:

1. En el grupo de trabajo de Optivity en windows, seleccionar el icono BootP/TFTP
2. Seleccionar el menu "EditFile"
3. Recordar aquí que los cambios a este archivo no pueden ser usados dinámicamente por sólo teclear "Yes".
4. Respaldar el archivo BOOTPTAB.TXT para salvar estos cambios.

Si no se desea comenzar BootP/TFTP, se puede accesar al archivo BOOTPTAB.TXT se deberá seguir los siguientes pasos:

1. Abrir el accesorio "Notepad" del programa de accesorios de windows
2. Cargar el archivo BOOTPTAB.TXT del directorio COMM
3. Respaldar los cambios hechos



Parámetros importantes del BOOTPTAB.TXT :

	hostname	Campo designado para el dispositivo para el cual se esta creando un registro
ht=	hardware type	Este campo es el tipo de hardware de red usado
ha=	hardware address	Este campo es la dirección MAC del NMM
tc=	template record	El valor en este campo puede a contener otros campos predefinidos
ip=	host IP address	La direccidon IP del dispositivo de donde será reinicializado
hd=	home directory	Este campo es la ruta del directorio en donde se encuentran las imagenes
bf=	bootfile	Es el campo del nombre del archivo de configuración

5.8.2 Modificación del archivo de configuración del NMM

Para modificar los archivos ".CFG" para cada módulo NMM que usa el BooTP, seguir los siguientes pasos:

1. Usar un editor de texto para construir un archivo de configuración boot que el módulo NMM pueda usar.
2. Seleccionar "OPEN" del menu "FILE" y y bajo del directorio COMM seleccionar el archivo ".CFG" a modificar
3. Hacer las modificaciones convenientes
    a. Nombre de la imagen.- teclear aqui el nombre de una imagen tal como 331x520.img
    b. Netmask (algo parecido como una máscara de la subred), sólo se se especifica
    c. Si se necesita un ruteador de default, teclar su dirección IP
    d. Agent-Key.- si se esta utilizando un agente avanzado, teclear la llave que fue asignado al NMM
    e. Salvar el archivo
    f. Salir del editor de texti

Una vez creado el archivo de configuración para el NMM, hay que dar una reinicialización al dispositivo:

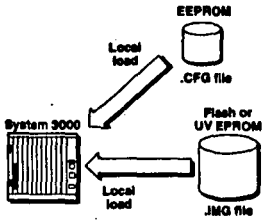
a. Dando un doble click al icono BooTP/TFTP

b. Dando una reinicialización directa al dispositivo

5.8.3 Configurando un módulo NMM para que reinicialice por si mismo

Para configurar un NMM que reinicialize por si mismo seguir los siguientes pasos:

1. Crear una entrada para el dispositivo en el archivo BOOTPTAB.TXT
2. Modificar o crear un archivo ".CFG" para el dispositivo que incluya lo siguiente:
    a. Especificar que use el modo de boot local y modo cargar
    b. Dar la llave del agente si es que el NMM usa un agente avanzado



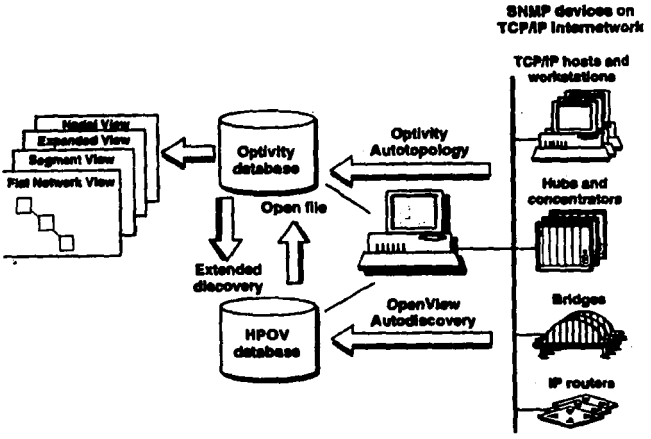
c. Dar la máscara de la subred

d. Salvar y cerrar el archivo ".CFG"

e. Arrancar Bootp/TFTP

f. Dar una reinicialización al módulo NMM

5.9 AUTOPOLOGIA OPTIVITY



La autopología Optivity encuentra dispositivos de red para obtener información de direcciones IP de NMM's, controladores de grupo, y SNMP basados en dispositivos de interconexión de redes. Los agentes basados en IP envían al plano de la red "hellos" (prueba de comunicación) y segmentan "hellos". Las tablas creadas para este intercambio de mensajes habilitan la aplicación del administrador de red Optivity para construir pantallas dinámicas, las cuales son actualizadas por la opción de "Validate" la cual es seleccionada por un mapa en

particular. Por esta razón, Optivity debe de actualizar sus mapa estáticos, a menos que los cambios hayan ocurrido desde que los mapas de "Open View" fueron generados.

La información acerca de los nodos es agregada a la base de datos de Optivity cuando se corre la pantalla a nivel de nodo para un segmento en específico, o cuando se selecciona la opción de "Node Discovery" del menú de aplicaciones.

El módulo NMM puede ser manualmente agregado cuando se añade un símbolo de una subred a un mapa de Open View, o este será seleccionado automaticamente durante la inicialización de Optivity. La autopología requiere que todos las configuraciones NMM deben de tener el mismo SNMP para cada red.

5.10 COSTOS Y BENEFICIOS

5.10.1 Pauta para la elección del concentrador

Una red proporciona muchas características para mejorar la productividad, reducir costos y permitir el intercambio de información importante. El que la red satisfaga estas necesidades lo determina una buena planeación previa a su instalación. Las necesidades de red actuales y futuras determinan lo extenso que debe ser el proceso de planeación. Las redes pequeñas de unos cuantos nodos, ubicadas en la misma área física, requieren una planeación mínima, en cambio, una planeación más amplia es obligada para aquellas redes de una cantidad enorme de nodos a situarse en diferentes espacios y hasta en diferentes pisos, redes que probablemente requerirán nodos adicionales en el futuro.

Una consideración importante cuando se planea la red es determinar cúantas computadoras se necesitan conectar de inmediato y en el futuro. El número máximo de nodos conectados en una configuración de red depende

de varios factores, incluyendo el sistema operativo de red, la topología física y el tipo de red. Estos factores también determinarán el tipo de concentrador a utilizar.

Los requisitso de rendimiento de la red dependen de varios factores, cada sistema operativo se comporta diferente, y algunos pueden ser más adecuados para determinar estándares de rendimiento que otros. Afectan el rendimiento el tipo de adpatador de red, la topología de la red, protocolos y el tipo de controlador a utilizar.

Si el objetivo principal de la red es compartir impresoras, entonces es probable que la configuración de red con menor rendimiento sea más que suficiente, en este caso el concentrador no tiene que ser de tipo modular ya que sería un costo bastante elevado el que se tendría que pagar.

Si se van a compartir archivos y datos con otros nodos de la red, si importa el rendimiento, por lo tanto, se debe pensar en una red que tenga el rendimiento de 10 Mb/s mínimo, como el de Ethernet, así como un concentrador de tipo modular que permita la transmisión de información eficiente.

El costo es un factor importante en la determinación de cúal de los requisitos de red especificados tiene prioridad y cuáles no. Los costos en los que se incurre para poner en funcionamiento diversas carcateristicas de red no están tan relacionados a todas las funciones sino a la tecnología disponible para ejecutar la función requerida. Por consiguiente, es muy posible que resulte excesivo el costo de poner en funcionamiento lo que parecería una tarea trivial y, en cambio, sea relativamente bajo el de poner en acción algo que parecía una tarea complicada.

En razón de los costos, tal vez se escoja dar prioridad a las necesidades establecidas y posteriormente poner en funcionamiento determinadas características. Todavía querrá asegurase de que el sistemas operativo escogido y el hardware de red podrían ser mejorados después de ejecutar las funciones diferidas. Ya que el costo disminuye

conforme la tecnología avanza, quizás se beneficie demorar el poner en funcionamiento características que no son de alta prioridad.

5.10.2 Procedimiento para la elección

La elección del concentrador se realiza mediante un concurso entre diferentes proveedores. Este concentrador se eligió de acuerdo a un concurso realizado para la elaboración de un cableado estructurado en un edificio con un total de 650 servicios de voz/datos, en el cual se incluía el tipo de concentrador a seleccionar.

Las características que se definieron para la elección del concentrador se tiene lo siguiente:

a) Tipo de Frame a utilizar
b) Cantida y tipos de protocolos de red a soportar
c) Número máximo de servicios
d) Velocidad en la transmisión de información
e) Tipo de software de monitoreo a utilizar
f) Costo
g) Soporte Técnico
h) Garantía

Se realizó un cuadro comparativo de los diferentes productos que presentarón los diferentes proveedores en concurso en el que se analizó cada uno de los puntos mencionados anteriormente. Resultando seleccionado el manejador Lattisnet SynOptics de la serie 3000.

5.10.3 Beneficios

Entre los beneficios que se tiene con la adquisición del manejador Lattisnet son :

1. Una amplia cantidad de servicios a usuarios
2. Menor tráfico en la red
3. Prevención de errores en la transmisión de información
4. Estadísticas del comportamiento de tráfico en la red
5. Repartición de tráfico a través del NMM
6. Transmisión de información de 10 Mb/s y tiende a 100 Mb/s
7. Si un módulo se daña se remplaza la pieza estando conectado al controlador sin interrumpir a los demás modulos su funcionamiento

5.10.4 Comparación con otro dispositivo de red en cuanto a costo

Se pretender dar servicio de red a 300 usuarios en un edificio, se desea adquirir el controlador lattisnet contra un hub Black Box . De estos dos se tiene lo siguiente:

Los costos están dados en dolares.

Par el controlador Lattisnet se tiene lo siguiente:

ELEMENTOS	COSTO	NUMERO	Total
Chassis del controlador	$1200	1	$1200
Módulo abastecedor de energía 3002	$1388	1	$1388
Módulo 3307 para 24 puertos	$2110	13	$27430
Módulo Administrador 3314	$2478	1	$2478
Módulo switching (opcional) 3328	$3030	1	$3030
			$35526

Para hubs Black Box se tiene lo siguiente:

ELEMENTOS	COSTO	NUMERO	TOTAL
Hub Black Box	2995	25	$74875
Conector	20	25	$500
			$75375

Como se observa es más barato el concentrador lattisnet al blackbox, además que no se incluye aquí el costo del cableado.

Como se ve es más facil concentrar a los nodos en un sólo módulo, a tener 25 hubs conectados juntos, además que según las mormas, no se pueden conectar más de 5 hubs consecutivamente, lo que es otras desventaja.

CONCLUSIONES

El hecho de valerse de una herramienta tan versátil como lo es la red, implica contar también con los elementos adecuados como el mantenimiento regular y precisa que se requieran.

El controlador Iattisnet como se vio en el desarrollo de este tema, nos permite monitorear a nivel de hardware todos los componentes que se ven o están involucrados en la red Lan en el cual esta instalado.

Este concentrador y con la ayuda del software Optivity, el cual es instalado en un nodo y que sirve como consola de monitoreo, nos permite obtener toda la información necesaria para la realización de estadísticas del comportamiento de la LAN, así como observar en donde se esta presentando un problema en la LAN ya sea en algún nodo o en algún componente que forma parte de la LAN.

Esta tecnología si bien en el mercado es costosa para instituciones educativas e inclusive para algunas empresas, de alguna forma tener ests controlador permite mantener en buen funcionamiento de la LAN así como el monitoreo constante de la misma.

Aunque resulta interesante mencionar, que aunque se tenga un buen equipo de monitoreo así como de los componentes de la LAN, se tiene una muy mala instalación de cableado estructurado, esto no funcionará correctamente y a la larga sería un costo demasiado elevado. Hay que recordar que el cableado estructurado es una de las partes fundamentales de una red, si la instalación fue pésima se tendrá constantemente errores en las transmisiones de señales y por lo tanto en el monitoreo ya que siempre detectará fallas en los nodos e inclusive de segmentaciones, y estos produce un costo elevado para la empresa.

El concentrador lattisnet es un buen elemento de la red, ya que en este mismo se tiene a la vez: puentes, ruteadores, conmutadores e inclusive la administradora de red que llevan a cabo el control de los diferentes cambios que se hagan en la misma.

Si bien la tecnología en comunicaciones avanza constantemente, el concentrador lattisnet modelo 3000 tiene aún un periodo de vida de 5 años más en el mercado, actualmente se habla ya de la nueva tecnología de la serie 5000 del mismo equipo, en los cuales ya se hablan de transmisión de información hasta de 150 Mb/s, más sin embargo, en México la mayoría de las empresas manejan su tecnología o transmisión de información a 10 Mb/s, aunque existen empresas como TELMEX que ya se esta actualizando al respecto y ya cuenta con equipo con transmisión de información de 150 Mb/s.

Como se planteo en el capítulo de introducción se cumplieron tanto el objetivo principal así como los particulares. Ya que se describió las características y funciones de cada uno de los elementos que conforman al controlador lattisnet, así como la forma en que trabajan cada módulo. Así como se describió la forma como interactua el programa Optivity con el controlador.

También se observó que es más facil de usar este tipo de controlador y el costo es mucho más bajo que el usar hubs de uso común, además de que estos hubs son de tipo no modular. A demás que el controlador lattisnet trabaja en conjunto con el software de administración Optivity como monitoreo. Aunque los hubs se pueden monitorear a través de estaciones de trabajo es de menor precisión. Además en lattisnet se puede seguir trabajando si alguno de sus segmentos no esta funcionando, no interfiere con los demás, y en cambio los hubs no realizan esta caracteristica en particular.

FIGURA A

Abastecedores de energía

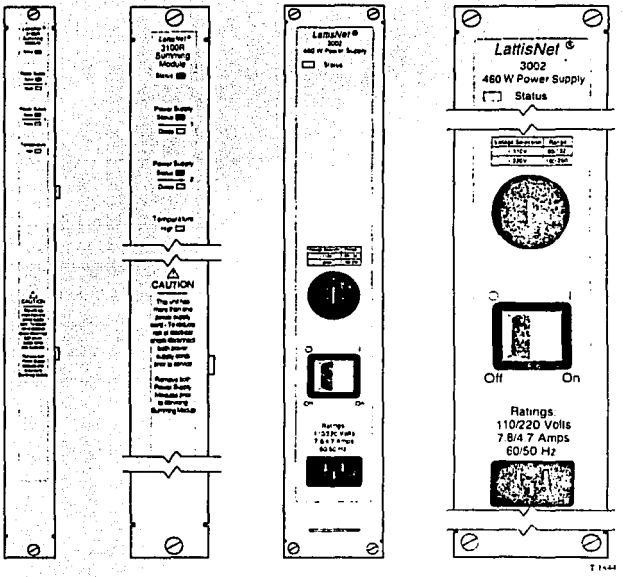


FIGURA B

MODULO DEL MANEJADOR LATTISNET SYNOPTICS SYSTEM 3000

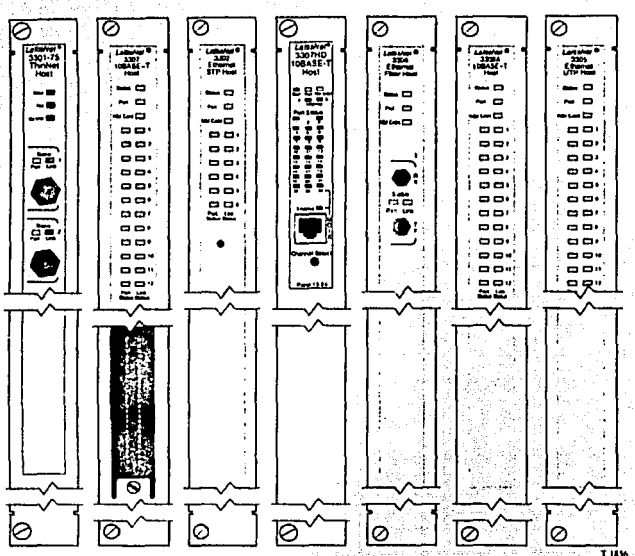


FIGURA C

MODULO MODELO 3308A 10BASE-T HOST

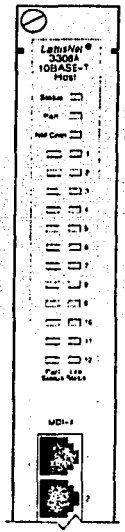


FIGURA D

MODULO MODELO 3307 50-PIN 10BASE-T HOST

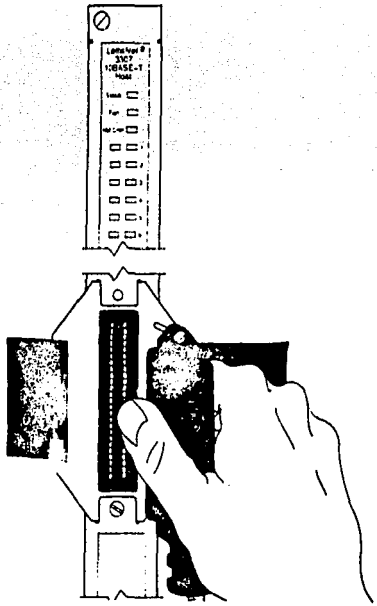


FIGURA E

MODULO MODELO 3307 HD 10BASE-T HOST

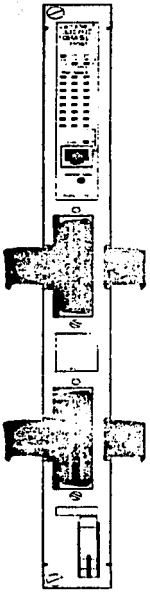


FIGURA F

MODULO MODELO 10BASE2 HOST

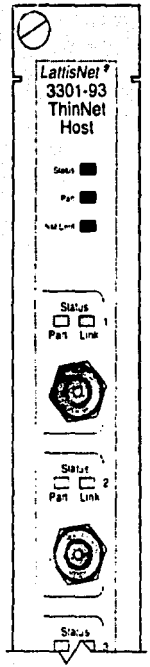


FIGURA G

MODULO MODELO 3302 STP HOST

FIGURA II

MODULO MODELO 3304 ST FOIRL HOST

FIGURA 1

MODULO MODELO 3305 UTP HOST

FIGURA J

MODULO MODELO 3368 LATTISSECURE HOST

FIGURA K

MODULO MODELO 3333 Y 3334-ST RETIMING

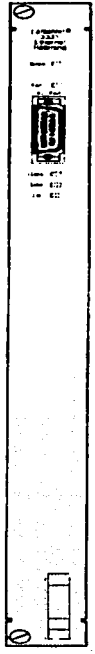


FIGURA L

MODULO ADMINISTRADOR DE RED MODELO 3331xA Y 3331xS

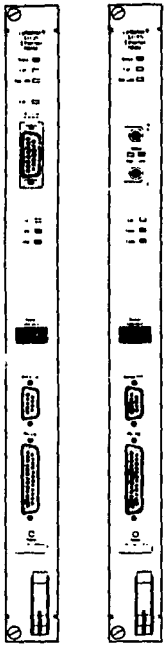


FIGURA M

MODULO BRIDGE MODELO 3323S Y 3324S-ST

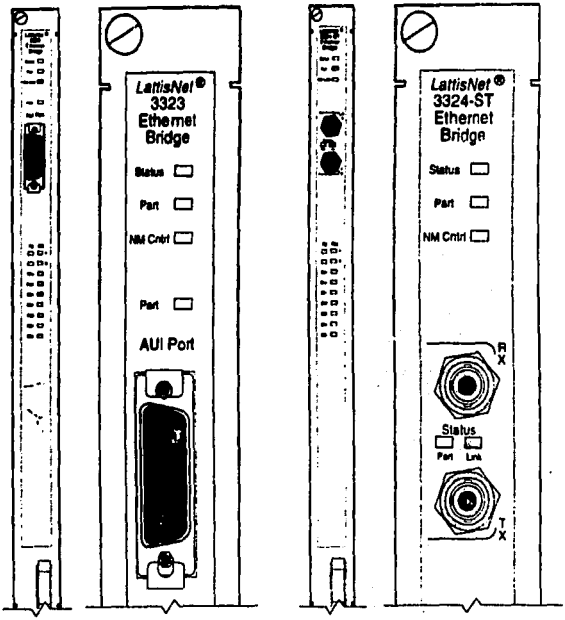
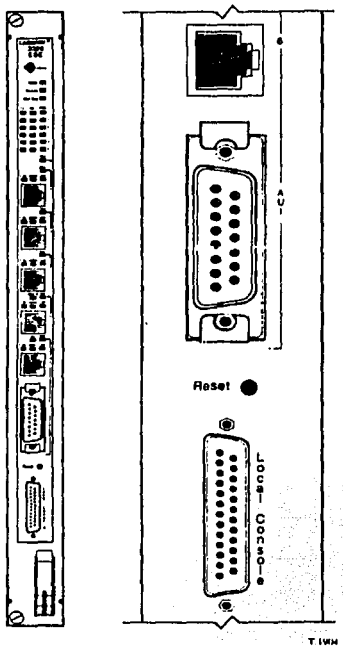


FIGURA N

MODULO MODELO 3328 ESE



10BASET .- especificación IEEE 802.3 que emplea cable par trenzado simple y que funciona a 10 Mbps.

10BASE2.- la implementación de Ethernet del estándar del IEEE 802.3 en cable coaxial delgado. También se le conoce como thin Ethernet o Thin Net, corre a 10 MB/s. Máxima longitud por segmento: 200 metros.

Administración de cuentas.- Una de las cinco categorías de administración de redes definidas por ISO para el manejo de redes OSI. Los subsistemas de administración de cuentas son responsables de recolectar los datos de la red que se refieren al uso de los recursos.

Address (dirección) .- En materia de redes, es una identificación única asignada a un dispositivo de la red de modo que pueda enviar y recibir mensajes independientemente.

Agente.- software que procesa pedidos y devuelve respuestas en alguna aplicación. En los sistemas de administración de redes los agentes residen en todos los dispositivos bajo control y reportan los valores de las variables especificadas a las estaciones de administración.

Algoritmo.- una secuencia finita de pasos dirigidos a realizar una tarea específica (método de solución).

Amplitud.- distancia entre los puntos alto y bajo de una forma de onda o una señal.

Ancho de banda.- la diferencia entre la frecuencia más alta y la más baja de un canal de transmisión, expresada en Hertz (Herts = ciclos por segundo).

ANSI.- American National Standards Institute (Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos.

ARP.- "Address Resolution Protocol". Proceso TCP/IP que mapea el protocolo internet direccionado a la dirección física de Ethernet.

ARPA.- "Advanced Research Projects Agency", agencia dentro del departamento de defensa de E.U. que da soporte a la red ARPANET.

ASCII.- American Standard Code for Information Interchange.- código de ocho bits para representar caracteres que emplea siete bits más paridad.

Asíncrona.- forma de transmisión que no requiere que el receptor y el transmisor mantengan "sincronía" sus relojes. Pero en cambio necesita que el transmisor "inserte" bits antes y después del caracter para que el receptor lo reconozca.

Atenuación.- reducción de la potencia de una señal eléctrica durante la transmisión. Medida en decibeles.

ATM.- (Asynchronous Transfer Mode; modo de transferencia asincrona) tecnologia de punta de transmisión y commutación a grandes velocidades por medio del movimiento asincrono de paquetes con rapidez.

ATDM.- (Asynchronous Time Division Multiplexing ; Multiplexor asincrona por división de tiempo). Método de envió de información que emplea el multiplexaje usual por división de tiempo (TDM), pero en donde se asignan ranuras de tiempo cuando se requiere, en lugar de preasignarlas a transmisores especificos.

AUI.- (Attachment Unit Interface; Unidad de interface de conexión) Tipo de conector que permite la conexión de un tipo de cable a otro a través de convertidores.

Backbone network.- actúa como conducto primario (o "espina dorsal") de tráfico que usualmente viene de, o va hacia, otras redes.

Baund.- unidad de velocidad de señalización igual al número de condiciones discretas o sucesos en la señal por segundo. Los bauds son equivalente a los bits por segundo cuando cada suceso en la señal representan exactamente un bit.

Baudio.- medida de la velocidad de transmisión de datos. La velocidad en baudios es igual al número de veces que cambia la condición de la linea por segundo.

BIOS.- (Basic input/Output System; sistema de entrada/salida básico), servicios de software y/o firmware que define la forma en que interactuan las aplicaciones y todos los puertos seriales y paralelos de entrada/salida.

Bit.- esun digito binario, puede ser 0 o 1. Es la unidad más pequeña de información que indica dos estados "off (0) y on (1) ".

Bit de paridad.- método sencillo para detectar errores en la transmisión. Se agrega un bot en 0 o 1 dependiendo del número de unos qie tenga el patrón a enviar.

BNC connector.- conector BNC, conector estándar empleado para ligar el cable coaxial IEEE802.3 10BASE2 a un receptor o transmisor.

Boot.- proceso de carga de los programas básicos para encender la computadora.

BootP.-protocolo que se utiliza para transferencia de información de inicialización (booting), entre un Boot-server y el dispositivo.

Bps.- abreviación de bits por segundo. La medida de velocidad de transmisón más utilizada.

Bridge (puente).- puente, dispositivo que permite enviar datos de una red a otra.

Bus.- es un circuito de transmisión eléctrica que sirve para transportar información entre varios dispositivos de una computadora.

Byte.-término genérico que se refiere a una serie de dígitos binarios consecutivos con los que se trabaja como si fuera una unidad, usualmente los 8 bits representan un caracter en binario.

Cable.- medio de transmisión que consiste en alambres o fibras ópticas envueltas por una cubierta protectora.

Cable coaxial.- un tipo de cable eléctrico en el cual un alambre sólido de metal es cubierto por un aislante, todo el cual es protegido por una malla de metal cuyo eje de curvatura coincide con el del alambre.

Canal.- un camino físico o lógico que permite la transmisión de información. En algunos casos puede ser sinónimo de Bus.

Carrier (portadora).- una forma de onda continua (normalmente eléctrica) cuyas propiedades le permiten ser modulada o alterada por una segunda que "porta" información.

CCITT.- "Comite Consultivo Internacional de Telegrafía y Telefonía". Fija estándares internacionales en comunicaciones.

Cliente.- nodo o programa de software que requiere servicios de un servidor.

Colisión.- el resultado de que dos o más estaciones traten de usar simultáneamente un medio de transmisión (cable) común.

Concentrador.- para fines generales, es una caja que concentra (de ahí su nombre) segmentos de cable de una red local para su mejor distribución y administración.

Conectividad.- estado que permite la transferencia de señales eléctricas desde un origen hasta un destino.

Conector.- es un accesorio al final de un alambre o conjunto de alambres que facilitan su conexión a un recurso.

CSMA/CD.- "Carrier sense Multiple Access/Collision Detection". Técnica utilizada para enviar señales dentro de una red local. El cable se utiliza por "competencia", y cuando una tarjeta detecta sólo la portadora, empieza a transmitir, pero debe seguir escuchando por si ocurre alguna colisión. De ser así, requiere hacer una retransmisión.

Datagrama.- un método de transmisión en el cual las secciones de un mensaje son transmitidas en cualquier orden, y el orden correcto se reestablece en la estación que recibe. Paquetes de datos que viajan individualmente, es decir, sin que exista una conexión.

Dispositivo.- entidad que puede tener acceso a la red. Se emplea en forma intercambiable con nodo.

DNA (Digital Network Architecture; Arquitectura de red digital).- arquitecturas de las redes de la compañía Digital Equipment Corporation.

Dominio.- en SNA es un SSCP y los recursos que controla; en IS-IS, un conjunto lógico de redes'

DTE (Dato terminal equipment, Equipo de terminal de datos).- parte de una estación de datos que sirve como fuente o destino de los datos, o ambos, y que ofrece las funciones de control de comunicacion de datos de acuerdo con los protocolos.

EBCDIC (Extended Binary Coded Decimal Interchange Code).- código de 8 bits desarrollado por IBM para representación de datos en sus grandes sistemas de computo.

EIA.- "Electronics industries association; asociación de industrias electrónicas", instituto que elaboró el estándar de comunicaciones RS 232C.

Colisión.- el resultado de que dos o más estaciones traten de usar simultáneamente un medio de transmisión (cable) común.

Concentrador.- para fines generales, es una caja que concentra (de ahí su nombre) segmentos de cable de una red local para su mejor distribución y administración.

Conectividad.- estado que permite la transferencia de señales eléctricas desde un origen hasta un destino.

Conector.- es un accesorio al final de un alambre o conjunto de alambres que facilitan su conexión a un recurso.

CSMA/CD.- "Carrier sense Multiple Access/Collision Detection". Técnica utilizada para enviar señales dentro de una red local. El cable se utiliza por "competencia", y cuando una terjeta detecta sólo la portadora, empieza a transmitir, pero debe seguir escuchando por si ocurre alguna colisión. De ser así, requiere hacer una retransmisión.

Datagrama.- un método de transmisión en el cual las secciones de un mensaje son transmitidas en cualquier orden, y el orden correcto se reestablece en la estación que recibe. Paquetes de datos que viajan individualmente, es decir, sin que exista una conexión.

Dispositivo.- entidad que puede tener acceso a la red. Se emplea en forma intercambiable con nodo.

DNA (Digital Network Architecture; Arquitectura de red digital).- arquitecturas de las redes de la compañía Digital Equipment Corporation.

Dominio.- en SNA es un SSCP y los recursos que controla; en IS-IS, un conjunto lógico de redes'

DTE (Dato terminal equipment, Equipo de terminal de datos).- parte de una estación de datos que sirve como fuente o destino de los datos, o ambos, y que ofrece las funciones de control de comunicacion de datos de acuerdo con los protocolos.

EBCDIC (Extended Binary Coded Decimal Interchange Code).- código de 8 bits desarrollado por IBM para representación de datos en sus grandes sistemas de computo.

EIA.- "Electronics industries association; asociación de industrias electrónicas", instituto que elaboró el estándar de comunicaciones RS 232C.

EISA.- "Enhanced International Standard Arquitecture; arquitectura estándar internacional" tipo de canal de 32 bits en la arquitectura de motherboards, tarjetas, etc.

Emulación.- la imitación que hace un dispositivo de otro. Tipicamente una PC actuando como terminal de un equipo mayor.

Estádar.- especificación que debe utilizar un sistema para cumplir con las caracteristicas que exige el mercado si es que quiere ser compatible y lograr la comunicación.

Estación de trabajo.- cualquier equipo conectado a una red, con capacidad propia de proceso.

Ethernet.- el estándar de tarjetas de red más conocido y sólido. Define una velocidad de transmisión de 10 Mb/s, utilizando protocolo CSMA/CD.

FDDI (Fiber Distributed Data Interfase; interfase de datos distribuidos por fibra).- estándar para transmisión de datos en redes locales utilizando fibra óptica, a una velocidad de 100 Mb/s.

FDM (Frequency Division Multiplexing; Multiplexor por división de frecuencia).- técnica en la que en un solo cable se puede asignar a la información de múltiples canales un ancho de banda basado en la frecuencia.

Fibra óptica.- un medio de transmisión de datos que consiste en una fibra de vidrio (o de plástico). Una fuente luminosa (LEDs o Lasers) emite un haz de luz que se va reflejando dentro del cable gracias a los diferentes grados de refracción entre el material de la fibra y una cubierta similar.

File server (servidor de archivos).- computadora dedicada a compartir los archivos que tienen almacenados en su(s) disco(s) entre los usuarios de una red local.

Firmware.- conjunto d eprogramas requeridos para implementar una función especifica. Estos programas se encuentran almacenados en ROM.

FOIRL.- " Fiber Optic Inter-Repeater Link", enlace o interfaz hacia una red de fibra óptica.

Frame (marco d einformación) .- unidad de información del nivel 2 del modelo OSI. Usualmente un frame consta de tres partes: un Header (encabezado) que trae información de control, direcciones fuentes y destino, et. Un campo de información y un campo de CRC (verificación de errores).

Frame relay (retransmisión de marcos).- protocolo empleado en la interfaz entre dispositivo de usuario y equipo de redes.

Frecuencia.- medida en Hertz (Hz), es el numero de ciclos de una señal de corriente alterna por unidad de tiempo.

Frecuencia Modulada.- proceso en donde se varia la frecuencia de una señal analógica para poder transportar información digital.

FTP (File Transfer Protocol; Protocolo de transferencia de archivos).- protocolo de aplicación IP para transferir archivos entre nodos de la red.

Gateway (Compuerta).- dispositivo que permite conectar dos redes locales con diferentes protocolos.

Half duplex.- capacidad de transmitir datos en solo una dirección a la vez.

Hardware.- equipo físico, todos los componentes electrónicos y mecánicos de una red, como computadoras personales, tarjetas de red y cables.

Hexadecimal.- sistema numérico en base 16. Se utiliza para representar combinaciones de 4 bits simplificando de esta manera la representación general de instrucciones máquina o datos.

Host (anfitrión).- sistema de computo en una red. Es similar a los términos device (dispositivo) o nodo, excepto que usualmente implica un sistema de computo, mientras que dispositivo y nodo generalmente se aplican a cualquier sistema de red, que incluye terminal servers (servidores de terminales) y enrutadores.

ISA.- "International Standard Arquitecture; Arquitectura estándar internacional". Tipo de canal de 8 ó 16 bits en la arquitectura de motherboards, tarjetas, etc.

IEEE (Institute of Electrical and Electronic Engineers; Instituto de ingenieros electrónicos y eléctricos).- organización profesional que define estándares de redes.

IEEE 802.2.- protocolo LAN de IEEE que especifica la implantación de la subcapa de control de enlace lógico de la capa de enlace. Se encarga del manejo de errores, creación de marcos y flujos de control; es interfaz de servicio en la capa 3. Se emplea en redes LAN tales como IEEE 802.3 e IEEE 802.5

IEEE 802.3.- protocolo LAN de IEEE que especifica la implantación de la capa física y la subcapa MAC de la capa de enlace. Utiliza acceso CSMA/CD en varias velocidades usando varios medios físicos.

IEEE 802.4.- protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing sobre una topología de bus

IEEE 802.5.- protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing a 4 o 16 MBps sobre el cable de par trenzado blindado y es muy similar a Token Ring de IBM.

IEEE 802.6.- especificación IEEE de red de área metropolitana basada en tecnología DQDB.

Intel.- importante corporación fabricante de circuitos electrónicos (chips) entre los que destacan su familia de microprocesadores.

Internet.- termino empleado para referirse al sistema de interconexión de redes mas grande del mundo, que conecta miles de redes en todo el planeta y que desarrollo una cultura basada en simplicidad, investigación y estandarizacion fundamentada en el uso real.

Internetworking (interconexión de redes) .- termino genérico usado para referirse a la industria que surgió alrededor del problema de conectar redes. El termino se puede referir tanto a productos como a procedimientos y tecnologías.

Interoperabilidad.- capacidad para comunicar equipos de computación de diversos fabricantes mediante una red.

IP address (dirección IP).- es una dirección de 32 bits asignada a maquinas anfitrionas que emplean TCP/IP. La dirección se escribe como cuatro octetos separados con puntos, formados por la sección de la red, una sección opcional de subred y una sección del anfitrión.

IPX (Internetrworking Packet Exchange).- protocolo Novell de capa 3, similar a XNS e IP que se emplea en redes Netware.

ISDN (Integrated Services Digital Network ; Red Digital de Servicios Integrados).- protocolos de comunicación propuestos por las compañías telefónicas para lograr que las redes de teléfono transmitan datos, voz y otros materiales de la fuente.

IS-IS (Intermediate System to Intermediate System ; Sistema Intermedio a Sistemas Intermedio).- protocolo jerárquico de enrutamiento OSI de estado de enlace, casado en enrutamiento DECnet fase V, en donde los sistemas intermedios intercambian información basada en una sola métrica, para determinar la topología de la red.

ISO (International Organization for Standarization).- organización internacional responsable de una amplia gama de estándares, incluyendo aquellos relevantes para las redes.

Jabber (balbuceo).- condición de error en la cual un dispositivo de la red continuamente transmite "basura" a la red. En IEEE 802.3 se refiere a un paquete de datos cuya longitud excede a la prescrita en el estándar.

LAN (Local Área Network).- red que cubre un área geográfica relativamente pequeña.

Lan Manager.- sistema de archivos distribuidos desarrollado y manejado por Microsoft

Lan Network.- paquete de manejo Token Ring y source-bridge ofrecido por IBM. Normalmente opera en una PC y verifica los puentes de rutas fuente y los dispositivos Token Ring y puede pasar mensajes de alerta a NetView.

Lan Server.- sistema de archivos distribuidos derivado de Lan manager.

LED.- "Light Emitting Diode". Diodo que emite luz.

Línea.- en forma genérica se refiere a lo mismo que enlace . En SNA es una conexión a la red.

Link (enlace).- canal de comunicaciones de la red consistente en un circuito o trayectoria de transmisión, incluido el equipo existente entre el transmisor y el receptor.

Login.- acción de entrar a utilizar un host o servidor de red, establece una sesión de trabajo y es reconocido como usuario por el sistema operativo.

LU (logical Unit ; Unidad Lógica).- componente primario de SNA, es un puerto de software que se establece para llevar a cabo una sesión.

MAC (Media Access Sublayer).- como esta definida por la IEEE, se trata de la porción baja de la capa de enlace de datos del modelo OSI. La subcapa MAC se encarga de los asuntos de acceso al medio de comunicaciones, como por ejemplo determinar si se usara token passing o competencia.

MAP (Manufacturing Automation Protocol).- arquitectura de red creada por la empresa General Motors para satisfacer las necesidades especificas de la fabrica. Especifica una red local token-passing similar a IEEE 802.4.

Media (medios).- plural de medium, en ingles. Entorno fisico mediante el cual pasan las señales de transmisión. los medios usuales en redes son el par trensado, el cable coaxial, la fibra óptica y la atmósfera.

Mensaje.- agrupamiento lógico de información en la capa de aplicación.

MIC (Media Interfase Connector).- conector FDDI que es un estándar por default.

Motherboard (tarjeta madre).- la tarjeta de circuitos principal en una computadora personal, regularmente posee diversas ranuras (slots) para agregar tarjetas de memoria, monitor, disco duro, red, modems, mouse, etc.

Name server (servidor de nombres).- servidor que la red ofrece para resolver nombres de la red y asociarlos con localidades (direcciones) de la red.

NCP (Network Control Program).- en SNA, se refiera a los programas que asignan rutas y controlan el flujo de datos entre un controlador de comunicaciones

NET (Network Entity Title).- direcciones de la red definidas por la arquitectura de redes ISO y empleadas en redes basadas en CLNS.

NetBIOS (Network basic Input/Output).- interfaz de la capa de sesión para redes de PC, producida por IBM y Microsoft.

NetView.- arquitectura y aplicaciones relacionadas con manejo de redes IBM.

Netware.- desarrollado y distribuido por Novell Inc, se trata del sistema de archivos distribuidos mas popular en la actualidad. Ofrece acceso transparente a archivos remotos y muchos otros servicios distribuidos de redes.

NFS (Network File System).- es un conjunto de protocolos de sistemas de archivos distribuidos desarrollado por la empresa Sun Microsystems, que permite el acceso remoto a archivo en una red.

NIC (Network Institute Controller).-controlador de interfaz de red, o tarjeta de interfaz de red.

Nodo.- termino genérico que se refiere a una entidad que puede tener acceso a una red.

NOS (Network Operating System).- termino genérico para referirse a lo que en realidad son sistemas distribuidos de archivos. Ejemplos de esto incluye NetWare, VINES de Banyan, NFS y LAN Manager.

OSI (Open System Interconnection).- interconexion abierta de sistemas. Programa internacional de estandarizacion, apoyado por ISO y CCITT, para desarrollar estándares para redes de datos. facilita la interoperabilidad de equipos hechos por diversos fabricantes.

Packet.- agrupamiento lógico de información que incluye un ncabezado (headre) y datos del usuario.

Patch Panel.- centro de parcheo. Administrador de cableado que puede contener regletas, hubs, etc, para la realización de un cableado limpio.

PCM (Pulse Code Modulation).- transmisión de información analógica en forma digital mediante muestreo y codificación con un numero fijo de bits

PDN (Public Data Network).- red operada por el gobierno o en forma privada para ofrecer comunicaciones por computadora al publico, normalmente cobrando una cuota.

PPP (Point-to-point).- protocolo de punto a punto, este protocolo ofrece conexiones de enrutador a enrutador y de anfitrión a red empleando circuitos sincrónicos y asincronismos.

Protocolo.- conjunto de reglas convencionales, utilizado para comunicar dos dispositivos de la misma naturaleza.

Red.- conjunto de computadoras enlazadas por algún tipo de cable.

Repetidor.- dispositivo que retransmite y amplifica la señal recibida. Actúa solamente en el nivel 1 del modelo OSI.

RJ-45.-conector para cable de par trenzado (UTP y STP).

RS-232C.- interfaz estándar para conectar un DTE a un DCE. la especificación técnica ha sido publicada por la EIA. Tradicionalmente usa 25 pines.

Ruteador.- dispositivo que toma un paquete (nivel 3 del modelo OSI) y lo envía del punto A al punto B, después de analizar cual es el camino óptimo para llegar a su destino. Esto se logra a la información que cada ruteador almacena sobre todos los nodos de la red.

Segmento.- termino usado en la especificación de TCP para describir una unidad de información de la capa de transporte.

Server (servidor).- nodo o programa de software que ofrece servicios a un cliente.

Sesión.- conjunto de transacciones relacionadas que suceden entre dos o mas dispositivos de la red. E SNA, es una conexión lógica que permite a dos unidades NAU comunicarse entre si.

Shielded.- cable con una capa de aislamiento para reducir la interferencia electromagnetica (EMI)

SNA (Systems Network Architecture).- arquitectura grande, compleja y con múltiples características desarrollada en la década de los 70's por IBM.

SNMP.- "Simple Network management Protocol". Protocolo estándar de la familia TCP/IP, enfocado al manejo, administración y control de redes que utilizen TCP/IP.

Socket.- estructura de software que opera como punto final de comunicaciones en un dispositivo de red.

TCP/IP.- juego de protocolos creados en los 70's por Vincent cerf. El objetivo era lograr protocolos independientes del hardware. Hoy en día, son los protocolos que permiten la mayor conectividad entre los más diversos equipos.

TCP.- "Transmission Control Protocol". Nivel 4 de la familia TCP/IP, es un protocolo orientado a conexiones, que garantiza la llegada de paquetes y su ordenamiento.

Telnet.- protocolo estándar internet de emulación de terminales

Terminal server.- procesador de comunicaciones que conecta dispositivos asincronicos a una red LAN o WAN mediante software emulador de terminales y de redes.

TFTP.- "Trivial File Transfer Protocol". Protocolo de trasnferencia de archivos basados en UNIX

Token.- marco de información de control cuya posesión da a un dispositivo de la red el derecho a transmitir.

Token-Ring.- red local diseñada por IBM. Está creada para conectar diferentes tamaños de equipos. Se basa en que el token pueda circular de nodo en nodo, a través de un anillo. Para enlazar los equipos e ir cerrando el anillo se utilizan MSAUs.

Topología.- descripción de las conexiones físicas de una red. Generalmente se conoce con este nombre la forma en que se dispone el cable en una red local.

Transceiver.- en redes IEEE 802.3 es un dispositivo a través del cual podemos conectar la tarjeta de red al cable de transmisión. Se usa también para designar cualquier dispositivo que transmite y recibe.

UTP.- "Unshielded Twisted Pair". Par trensado no blindado

WAN (Wide-area Network).- red que ocupa in área geográfica amplia.

X.25 .- estándar del CCITT que define el protocolo de comunicaciones por el que una computadora pueda accesar una red de conmutación en paquetes. En general cuando se habla de X.25 se habla de una familia de protocolos que son: X.3, X.28, etc.

BIBLIOGRAFIA

BLACK, UYLESS. Data Networks: Concepts, Theory and Practice
Prentice Hall, 1989.

COMER,DOUGLAS. Internetworking with TCP/IP: Principles, protocols and Architecture
Prentice Hall, 1988

GONZALEZ, NESTOR. Comunicaciones y redes de procesamiento de datos
McGraw Hill , 1992

KUO.F.F. Protocols and Techniques for Data Communication Networks
Prentice Hall, 1981

LAM, S. Tutorial: Principles of Communication and Networking Protocols
IEEE Computer Society Press, 1984

SCHWARTS, M. Telecommunications Networks: Protocols, Modeling and Analysis
Addison-Wesley, 1987

SHERMAN, KEN. Data Communications: A User's Guide
Prentice Hall , 1990

SPRAGINS, E. Telecommunications Protocols and Designs
Addison-Wesley, 1991

STALLINGS, WILLIAM. Local Networks
Macmillan, 1990

SUNSHINE, CARL. Computer Network Architectures and Protocols
Plenum Press, 1989

TANENBAUM, ANDREW. Redes de ordenadores
Prentice-Hall, México 1990

ZIMMERMAN, H. "OSI Reference Model -The ISO Model of Architecture for Open Systems Interconnection" IEEE Transactions on Communications COM-28, No. 4, abril 1980.