88

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

"TCP/IP CARACTERISTICAS Y APLICACIONES MAS USUALES"

T E S I S

Que para obtener el título de

INGENIERO MECANICO ELECTRICISTA

p r e s e n t a

JESUS GERARDO RODRIGUEZ URBINA

ASESOR: ING. JOSE UBALDO RAMIREZ URIZAR

Cuautitlán Izcalli, Edo. de Méx. 2000

VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos el Trabajo de:

Tesis
"TCP / IP Características y aplicaciones más usuales".

que presenta el pasante: Rodríguez Urbina Jesús Gerardo
con número de cuenta: 9361656-6 para obtener el TITULO de:
Ingeniero Mecánico Electricista.

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutida en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO

A T E N T A M E N T E.
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Edo. de Méx., a 12 de Julio de 2000

PRESIDENTE	Ing.Jorge Buendía Gómez	
VOCAL	Ing.José Ubaldo Ramírez Urizar	
SECRETARIO	Ing.Juan González Vega	
PRIMER SUPLENTE	Ing.Petra Medel Ortega	
SEGUNDO SUPLENTE	Ing.José Luis Barbosa Pacheco	

Agradecimientos

Con el presente trabajo de tesis quiero agradecer al apoyo de mi mama Cristina Urbina B., a mis hermanas Rosalba Rodríguez U y Adriana Rodríguez U., el conocimiento que me fue brindado por los profesores y compañeros de trabajo, a mi asesor el Ing. J. Ubaldo Ramírez Urizar.

A Rosalba Mendoza Rivera y sus papas.

Y además en especial a **Delfina Urbina Becerra**, por todo su cariño.

Jesús Gerardo.

INDICE:

CAPITULO 1. CONCEPTOS GENERALES DE LAS REDES DE COMPUTADORAS.

Página.

CAPITULO 2. ESTRUCTURA DE UNA RDC.

CAPITULO 3. REDES TCP/IP.

CAPITULO 4. CONSIDERACIONES PARA EL DISEÑO DE UNA RED.

Objetivo.

Describir los conceptos principales, sus características y la configuración de los equipos utilizando el protocolo TCP/IP en las computadoras de usuario final.

JUSTIFICACION:

El presente trabajo se realiza en virtud de que la bibliografía que se encuentra con respecto al tema, en su mayor parte se encuentra escrita en idioma ingles y a la que podemos accesar en español esta escrita con un lenguaje muy técnico; el cual si no se cuenta con las bases necesarias es difícil de entender, por lo mismo surge la necesidad de recopilar de diferentes textos la información necesaria para dar a conocer algunos de los aspectos relevantes de este protocolo, el cual es muy utilizado en las comunicaciones vía Internet para la transmisión de datos de una manera eficaz y segura.

La presente tesis intenta describir los aspectos del protocolo de una manera sencilla (en la medida de lo posible) para que los estudiantes de la carrera de ingeniería aún sin contar con los conocimientos previos, puedan entender como funciona dicho protocolo y en dónde es aplicado; además de las ventajas que tiene sobre algunos otros.

INTRODUCCION

Dado que la tendencia actual de las telecomunicaciones es el uso de protocolos de alto rendimiento, como el TCP/IP, es importante que los estudiantes de la carrera de Ingeniería Mecánica Eléctrica (IME) conozcan los conceptos, características y configuración de las tecnologías involucradas (Software y Hardware).

Los estándares impiden situaciones en las cuáles dos sistemas, aparentemente compatibles, en realidad no lo sean. Por ejemplo, hace aproximadamente trece años, el disquete de 5.25 pulgadas venía en dos presentaciones de alta y baja densidad (esto nos proporciona diferente capacidad de almacenamiento de información en ellos), posteriormente se introdujo el disquete de 3.5 pulgadas con las mismas presentaciones alta y baja densidad pero en tamaño menor y con ello las unidades de lectura / escritura de alta y baja densidad, esto provoco que si en una máquina no se tenía una unidad de lectura / escritura de alta densidad no se podría accesar al disquete de alta densidad no así al de baja; debido a que estas unidades solo reconocen este formato haciendo con esto que se tuviera que cambiar estas unidades con el tiempo y la evolución de esta tecnología, sólo quedaron las unidades de disquete de 3.5 pulgadas en formato de alta densidad que es el utilizado hoy en día.

La creación de un estándar en el mundo de hoy no es cosa sencilla. Varias organizaciones están dedicadas a desarrollar estándares de una forma completa y clara. La más importante de ellas es la Organización Internacional para la Estandarización (Organitation International For Standardization), ISO. La ISO está compuesta de organizaciones de normas y estándares de muchas naciones, que intentan ponerse de acuerdo en un criterio internacional, varias son las Organizaciones e Institutos que son grupos miembros.

La organización de normas de cada nación puede crear un estándar para su país si así lo quisieran , sin embargo, la meta de ISO es decidir y ponerse de acuerdo sobre estas reglas a nivel mundial. De lo contrario, podrían existir incompatibilidades que no permitirían que el sistema de una nación fuera utilizado en otra.

La mayoría de los estándares se encuentran en lengua inglesa, esto puede causar confusión, en vista de que es un lenguaje incómodo; la razón de esto es que puede resultar difícil describir algo sin ambigüedades, y algunas veces se necesita de la creación de nuevos términos, que el estándar mismo define. No solo los conceptos deben quedar definidos con claridad, sino también el comportamiento absoluto. Sería sencillo definir un método de comunicaciones, como TCP/IP, si no fuera por la complicación de definirlo para

sistemas abiertos; el uso de un sistema abierto añade otra dificultad, debido a que los aspectos de estas normas deben ser independientes del tipo de máquina. Para ayudar a definir un estándar, por lo general se utiliza un método abstracto. A fin de describir sistemas de una forma abstracta, se necesita tener un lenguaje que cumpla con el propósito. Muchas organizaciones han desarrollado un sistema de este tipo; el más común, el Abstrac Syntax Notation One de ISO, abreviado como ANSI.1., está adecuado parta describir redes de sistemas abiertos.

El concepto primario de ANSI.1 es que cualquier dato, independientemente de tipo, tamaño, origen o propósito, se pueden representar por objetos que sean independientes del hardware, del software del sistema operativo o de la aplicación. Este sistema define el contenido del encabezado del protocolo de un datagrama la porción de información al principio de un objeto que se ocupa de describir el contenido del sistema-. Una parte de ANSI.1 describe el lenguaje utilizado para describir objetos y tipos de datos, otra parte se ocupa de definir reglas básicas de cifrado, que tratan del movimiento de los objetos de datos entre sistemas.

Estándares Internet:

Cuando en 1980 se estableció la Agencia de Proyectos de Investigación Avanzada de la Defensa (DARPA), se formó un grupo cuya meta era desarrollar un conjunto de estándares para Internet. El grupo llamado, Consejo de Control de Configuración Internet (ICCB), se reorganizó en 1983 para formar el Consejo de Actividades Internet (IAB), con la tarea de diseñar, ocuparse de la ingeniería y administrar Internet.

En 1986 el IAB pasó la tarea de desarrollar los estándares Internet al Grupo de Trabajo de Ingeniería Internet (IETF), en tanto la investigación a largo plazo fue asignada al Grupo de Trabajo de Investigación Internet (IRTF). El último paso fue la formación en 1992 de la Internet Society, donde al IAB se le cambió el nombre a Internet Architecture Board. Este grupo es responsable de los estándares existentes y futuros, y está subordinado al consejo de la Sociedad Internet (Internet Society).

Prácticamente desde el principio, Internet se definió como "*una colaboración internacional libremente organizada de redes autónomas interconectadas*" que soportaban comunicaciones de anfitrión a anfitrión; mediante adhesión voluntaria a protocolos y procedimientos abiertos, definidos en una publicación técnica conocida como Estándares Internet (Internet Standards).

El protocolo es un conjunto de reglas que se deben seguir a fin de entenderse dos o más partes que se encuentran interactuando; los protocolos en computación definen la forma como ocurren las comunicaciones; si una computadora envía información a otra y ambas siguen correctamente el protocolo, el mensaje pasará, independientemente del tipo de máquinas que sean y del sistema operativo que empleen; siempre que la máquina tenga software que el protocolo pueda manejar, las comunicaciones serán posibles. Esencialmente, un protocolo de computación es un conjunto de reglas que coordina el intercambio de información.

CAPITULO 1

CONCEPTOS GENERALES DE LAS REDES DE COMPUTADORAS.

En 1981 IBM presentó la computadora personal, esto estaba dirigido a personas que deseaban disponer de su propia computadora, los usuarios de estas comenzaron a conectar entre sí sus sistemas formando redes, de forma que podían compartir archivos y recursos como impresoras y otros periféricos; alrededor de 1985, las redes se hicieron tan grandes y complejas que el control lo debía tomar el departamento de informática. En la actualidad, las redes necesitan un control de seguridad, monitorización y administración, a menudo se extienden fuera de la oficina local, abarcando el entorno de la ciudad o uno mayor.

1.1. Definición de las redes:

La red más simple conecta dos computadoras, permitiéndoles compartir archivos e impresoras, una más compleja podría conectar todas las computadoras de una compañía en el mundo. Para compartir impresoras podrá bastar con un multiplexor, pero si deseamos compartir de manera eficaz archivos y ejecutar aplicación es de red, necesitamos tarjetas de red y cableado para conectar los sistemas, aunque se pueden utilizar los puertos serie y paralelo para realizar una interconexión, estos no ofrecen la velocidad e integridad que necesita un sistema operativo de red seguro y con prestaciones altas, que permitan manejar muchos usuarios y recursos.

Una vez realizadas las conexiones, se ha de instalar el sistema operativo de red: Existen dos tipos básicos de sistema operativo de red.

- **Punto a punto.** Este permite a los usuarios el compartir los recursos de sus computadoras y acceder a los recursos compartidos de las otras computadoras. Microsoft Windows para trabajo en grupo y Novell Lite son sistemas operativos punto a punto. El modo punto a punto implica que todas las computadoras poseen el mismo estatus en la red es decir, ningún sistema es *esclavo* del otro.
- **Con servidor dedicado.** En un sistema con servidor dedicado, una o más computadoras se reservan como servidores de archivos, no pudiendo utilizarse para nada más; los usuarios acceden a los directorios y recursos de los servidores de archivo dedicados, pero no a los de los otros sistemas, de esta forma se aumenta la seguridad y se evita la reducción del rendimiento de las computadoras personales. A estos sistemas se les denomina comúnmente como *cliente-servidor*.

En una red, cada computadora accede a los programas y archivos que se encuentran en un servidor central, pero ejecutan estos en su propia memoria y con su propio procesador. Las redes son *sistemas de procesamiento distribuido*, ya que cada computadora lleva a cabo su propio procesamiento, debido a esto el servidor no se sobrecarga debido a la tarea de procesamiento de cada computadora y se optimizan por tanto los servicios de archivo y red, así como el almacenamiento, tareas de gestión, monitorización, compartición de impresoras y seguridad.

1.2. Componentes de una red:

Una red está compuesta tanto de hardware como de software. El hardware incluye las tarjetas de red, como los cables que las unen; mientras que el software abarca los controladores (programas de gestión de los periféricos) y el sistema operativo que gestiona la red.

Los componentes se listan y describen a continuación como se muestran en la figura 1.

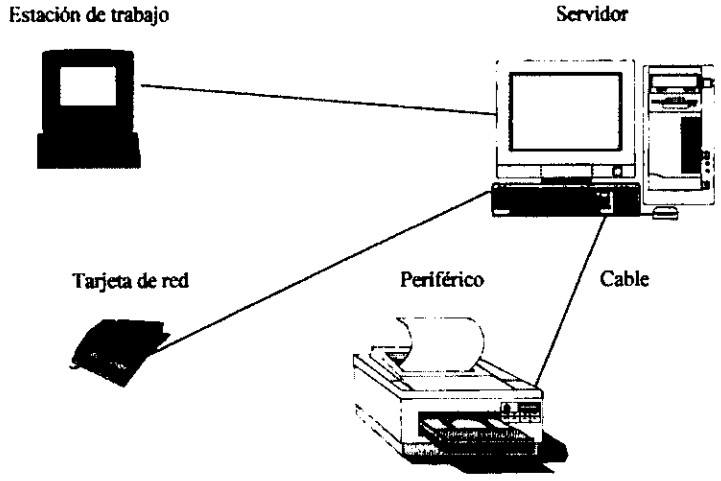

Figura 1. Componentes de la red.

- **Servidor:** El sevidor ofrece los servicios de red a las estaciones de trabajo, entre estos servicios se incluyen almacenamiento de archivos, la gestión de usuarios, la seguridad, las órdenes y opciones para los usuarios de red, las órdenes del responsable de la red y otros.
- **Estaciones de trabajo:** Cuando una computadora personal se conecta a la red, se convierte en un nodo de la red. Y se puede tratar como una estación de trabajo o *cliente*; estas estaciones son computadoras con

sistema DOS, UNIX, Macintosh de Apple, con OS/2 o estaciones sin disco.

1.2.1. Tarjetas de red:

Tarjetas de red: Para que la computadora se conecte a la red, necesita una tarjeta de red que soporte un Esquema de red específico, como Ethernet, ArcNet o Token Ring. El cable de red se conecta a la parte trasera de la placa. Existen redes sin cable, se conectan por radio o rayos infrarrojos.

También se encuentran tarjetas de red de diversos fabricantes, se pueden elegir entre distintos tipos, según se desee configurar o cablear la red; los tres tipos más usuales de red son: ArcNet, Ethernet y Token Ring, las diferencias entre estos tipos se encuentran, en el método y velocidad de comunicación, así como en el precio. Anteriormente (hace 4 años aproximadamente), el cableado estaba más estandarizado; ArcNet y Ethernet Usaban cable coaxial, y Token Ring usaba par trenzado, actualmente se pueden adquirir tarjetas que admiten diversos medios, lo que hace más fácil la planificación y configuración de las redes.

Hay tarjetas de red para equipos AT con conectores de bus de 8 ó 16 bits con arquitectura estándar de la industria (ISA), las tarjetas de 16 bits dan mejor rendimiento pero con mayor costo, también existen para sistemas con arquitectura microcanal (MCA), como los equipos PS/2 de IBM, y para equipos con bus de arquitectura estándar extendida de la industria (EISA), como el Compaq DESKPRO 486.

La tarjeta de red gestiona la comunicación entre las computadoras de red, según definen las normas de gestión del protocolo y de acceso al medio usadas por la tarjeta en particular; algunos fabricantes desarrollan placas que cumplen con las especificaciones básicas del tipo de red (Ethernet, Token Ring o ArcNet).

Las diferencias de diseño del hardware de las tarjetas pueden reducir el rendimiento de la red; por ejemplo, si una tarjeta con interfaz de 16 bits envía los datos a una tarjeta de 8 bits más rápido de lo que ésta los puede procesar, se debe montar memorias intermedias en las tarjetas de 8 bits para retener temporalmente la información.

Las tarjetas de red se suministran con un disco que contiene los archivos controladores, que son utilizados para configurar las tarjetas, tanto si son usadas en una estación de trabajo como en el servidor, mientras que las rutinas que codifican la información y la envían al cable se encuentran dentro de la tarjeta; el controlador define como se mueven los datos en la tarjeta y como se relaciona con los protocolos.

1.2.2. Cableado:

El cable coaxial fue uno de los primeros tipos que se usaron, pero el par trenzado (UTP), posteriormente fue ganando popularidad; el cable de fibra óptica (FDDI) es utilizado cuando es importante la velocidad. Si bien los avances en el diseño de las tarjetas de red permiten velocidades de transmisión sobre cable coaxial o par trenzado por encima de lo normal, actualmente el cable de fibra óptica es la mejor elección cuando se necesita una velocidad alta de transferencia de datos*, aunque se deben tomar en cuenta diversos factores antes de elegir el sistema de cableado para una red en concreto.

- **Sistema de cableado:** Este sistema está constituido por el cable utilizado para conectar entre sí el servidor y las estaciones de trabajo.
- **Recursos y periféricos compartidos:** Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de disco óptico, las impresoras, y todos los equipos que puedan ser utilizados por cualquiera en la red.

Al seleccionar el tipo de cable, hay que tomar en cuenta la seguridad y aislamiento del cable, el blindaje protege al cable coaxial de las interferencias, haciéndolo más fiable, pero más caro que el par trenzado, el cable de fibra óptica es seguro, ya que no emite ninguna señal que se pueda monitorizar, no necesitando blindaje, pero es el más caro; el cable de par trenzado ofrece cierta protección contra interferencias, pero sólo permite alcanzar distancias cortas entre las conexiones, pero últimamente se ha hecho popular debido a los avances de las técnicas de transmisión que la han permitido alcanzar la velocidad de transmisión Ethernet (10 Mbps), el cable Ethernet 10BASE-T es buena opción para las redes locales, pero requiere concentradores relativamente caros; una comparación de estos cables se muestra a continuación.

Variable	Par trenzado	Coaxial	Fibra óptica
Costo	Bajo	Moderado	Alto
Ancho de banda	Moderado	Alto	Muy alto
Longitud	Sobre 100 pies	Sobre 1,000 pies	Miles
Interferencia	Alguna	Baja	Ninguna
Fiabilidad	Alta	Alta	Muy alta
Velocidad	10 Mbps.	100 Mbps.	1 Gb en adelante.

*Aunque implica mayores costos generales.

Características del cable coaxial:

- Le afectan interferencias externas, por lo que debe estar blindado para reducirlas.
- Puede actuar como una antena conforme aumenta la distancia, captando ruidos e interferencias de motores, transmisores de radio y otras fuentes de potencia eléctrica.
- Tiene problemas con las conexiones a tierra.
- Emite señales que pueden ser registradas por personas no deseadas

Características del cable de fibra óptica:

Este cable es el más caro de los utilizados en las redes, aunque el aumento de la competencia ha reducido su precio.

- Se usa en combinación con otros tipos de cables, como una conexión central entre los servidores y segmentos de red local (Back Bone).
- Posee una mayor distancia potencial y velocidad de transmisión que los demás cables.
- No emite señales, y se puede usar en áreas de alta seguridad.
- No se ve afectado por el ruido eléctrico.
- Las conexiones no autorizadas en el cable se pueden detectar ajustando la cantidad de luz a lo largo del cable, si se produce una conexión, la línea fallará porque el sistema no estará ajustado a dicha conexión.
- Es más delicado.

Características del cable de par trenzado:

El cable de par trenzado es la opción más usual y tiene las siguientes características.

- Es el sistema de cableado más económico.
- Se pueden utilizar líneas telefónicas de par trenzado ya existentes.
- El par trenzado tiene limitaciones de distancia, pero se pueden corregir usando coaxial o fibra óptica para las conexiones centrales.
- Es susceptible a algunas interferencias externas.

1.3 Arquitectura de la red:

La arquitectura viene definida por su topología, el método de acceso a la red y el protocolo de comunicación. Los *métodos de acceso a la red* describen cómo puede acceder la estación de trabajo al cable, cuando otra estación lo está usando. El *protocolo* es la regla que controla la forma en que son transferidos los paquetes de información de una estación de trabajo a otra.

- **Método de acceso al cable:** Este describe cómo accede un nodo al sistema de cableado. Los sistemas de Cableado lineales, como Ethernet, pueden utilizar un método de detección de portadora, con lo que la estación comprueba el cable para saber si está siendo utilizado antes de transmitir. En este caso todos los nodos la reciben, siendo éstos los que determinan si la información va dirigida a ellos o no, si no fuera así, el nodo devuelve la información recibida; si dos nodos emiten al mismo tiempo se produce una colisión, debiendo volver a enviarla ambos después de esperar un tiempo fijado de forma aleatoria para cada uno; en este tipo de redes, el rendimiento se reduce cuando existe mucho tráfico.

  Las redes en anillo, normalmente utilizan un método de paso de testigo; con este sistema, una estación de trabajo sólo transmite cuando pose el testigo, este testigo es como un pase que permite utilizar la red. Cuando una estación está preparada para transmitir, ha de esperar a que este libre el testigo y apoderarse de el, así se evita que dos máquinas utilicen el cable simultáneamente.
- **Protocolos de comunicaciones:** Los protocolos de comunicaciones son las reglas y procedimientos utilizados en una red para establecer la comunicación entre los nodos que disponen de acceso a la red; los protocolos gestionan dos niveles de comunicación distintos, las reglas de alto nivel definen cómo se comunican las aplicaciones, mientras que las de bajo nivel definen cómo se transmiten las señales por el cable. Una vez definidos los protocolos, los fabricantes pueden diseñar y producir productos para red que funcionen en sistemas con elementos de distintos fabricantes.

1.3.1 Topología:

La topología de una red es la organización del cableado.

La *topología* define como se llevará el cable a cada estación de trabajo concreta, y tiene un papel importante en las decisiones a tomar sobre el cableado. Como se ve en la figura 2, una red puede tener una topología lineal, en anillo o en estrella, así se debe pensar cuál es el mejor método para realizar el cableado en el edificio. Actualmente, las decisiones se toman en función del costo, distancia del cableado y la topología.

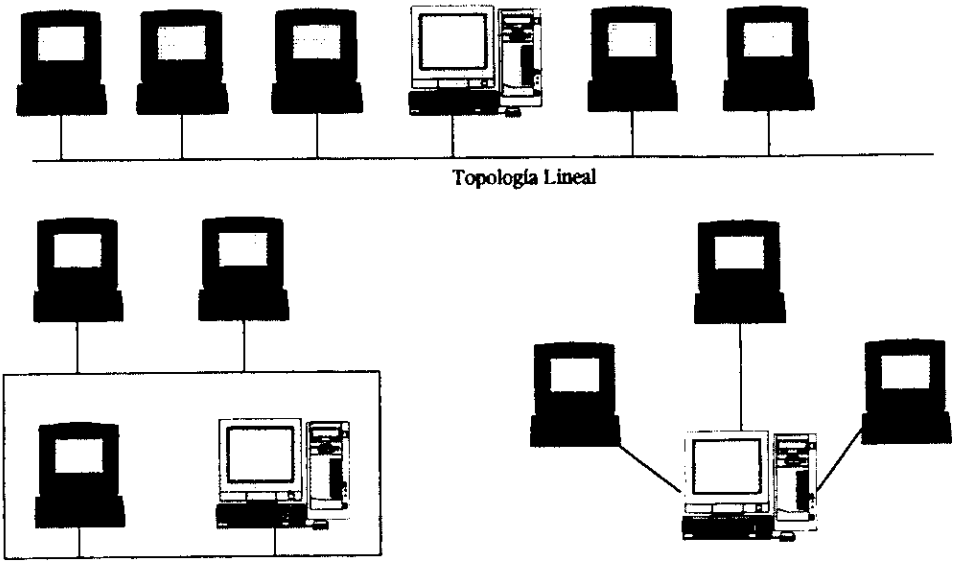

Figura 2. Topologías de red.

1.3.2 Tipos de red:

ArcNet: Este tipo de red utiliza una topología en estrella o en bus con un método de acceso por pase de testigo en banda base, usando cable coaxial a bajo costo, la velocidad de transmisión es de 2.5Mb/seg. ArcNet fue desarrollado por Datapoint en 1970, en 1981, Standard Microsystem Corporation (SMC) desarrolló el primer controlador de LAN en un chip basado en el protocolo por pase de testigo ArcNet; en 1986, se presentó un nuevo conjunto de chips que soportaban topologías en bus.

ArcNet está considerado generalmente como un sistema con un bajo rendimiento, pero soporta grandes longitudes de cable de hasta 600mts cuando se usan hubs activos, las nuevas versiones soportan fibra óptica y par trenzado, debido a lo flexible de su método de cableado, que permite grandes tramos y configuraciones en estrella en la misma LAN. ArcNet es una buena opción cuando la velocidad no es factor importante y sí el precio. Se ha desarrollado el ArcNetplus, una versión a 20Mb/seg de ArcNet compatible

con la anterior, ambas versiones pueden estar en la misma LAN. ArcNetplus soporta tamaños de paquete más grandes y más estaciones.

Hub activo (concentrador): Es un conmutador de red que acondiciona y amplifica la intensidad de la señal; las estaciones pueden estar a distancias de hasta 600 metros de concentradores activos, la mayoría tienen ocho puertos para conectar las estaciones u otros concentradores.

Hub pasivo: Es un concentrador de cuatro puertos con conectores BNC, usado como un centro de conexión y distribuidor de señales; las estaciones no pueden estar a más de 30 metros del concentrador, se deben utilizar acopladores en todos los puertos no usados.

Cableado ArcNet: El cableado usado es coaxial RG-62/U de 93 ohmios con conectores BNC. Los tipos de cable disponibles son cable antinflamable, cable para interior, cable subterráneo y cable aéreo.

Reglas y limitaciones aplicadas a las redes ArcNet:

- La mayor parte de los concentradores activos tienen ocho nodos y las estaciones conectadas a los hubs pueden estar hasta 600 metros de distancia del concentrador.
- Estos concentradores se pueden conectar para formar una configuración jerárquica; la distancia máxima entre dos de ellos es de 600 metros.
- Con un concentrador pasivo se pueden agrupar hasta cuatro estaciones, cada estación no puede estar a más de 30.5 metros de este.
- Los concentradores pasivos no pueden conectarse a otro pasivo, estos se pueden unir a otros concentradores activos a una distancia máxima de 30.5 metros.
- Los nodos no usados en los concentradores pasivos deben tener instalado un acoplador de 93 ohmios.
- La distancia máxima entre estaciones en extremos opuestos de la red es de 600 metros.
- Cuando las estaciones se cablean en una configuración de bus, la longitud máxima del tramo es de 30.5 metros.
- El número máximo de estaciones de trabajo es de 255.

La estación de trabajo con el número más bajo de dirección, difunde un testigo de permiso para cada estación de trabajo, con lo cual le concede permiso para acceder al cable, las otras estaciones acceden al cable según sus números de dirección.

Token Ring: Es una implementación en red de IBM basada en el estándar 802.5; es una red en anillo por pase de testigo que puede configurarse en una topología en estrella, se pueden conectar hasta ocho estaciones a un concentrador central, llamado unidad de acceso multiestación (MAU), si falla una placa de red, la MAU puentea inmediatamente la estación para mantener el anillo de la red, sin embargo, si falla una tarjeta de red, no es posible realizar el puenteo, interrumpiéndose la red; diversos fabricantes ofrecen productos que reducen el problema, pero necesitan de una conexión a una fuente de potencia, y son más caros ya que deben tener capacidades de gestión en situaciones de alerta.

Si se llega a romper un segmento de cable, en este tipo de red, se forma un anillo en sentido contrario utilizando un conjunto de hilos redundantes en los cables.

En la actualidad se ofrecen redes Token Ring, con métodos de conexión que superan al diseño de IBM; es común el par trenzado sin blindaje y las MAU con 16 puertos, detectores de fallos y utilidades de administración.

La MAU: Conecta hasta ocho estaciones usando cables adaptadores de red, se pueden conectar hasta doce dispositivos MAU. Los cables adaptadores tienen en un extremo un conector de 9 patillas para su conexión a la tarjeta de red, y en el otro un conector especial tipo A que los conecta con el MAU; estos cables tienen sólo 3 metros, pero se pueden utilizar cables prolongadores; estos cables extienden la distancia entre una estación y un dispositivo MAU, o entre dos MAU, deben ser de par trenzado blindado con hilos de 26 AWG y pueden tener hasta 50 metros, cuando se usan dividen por dos la distancia potencial de la estación a la MAU. El número máximo de estaciones en un anillo es de 260 para cable blindado y de 72 para cable de par trenzado sin apantallar, la distancia máxima de la estación a la MAU con cable apantallado conteniendo dos pares trenzados 22 AWG es de 101 metros, suponiendo que el cable es un segmento continuo; si los segmentos de cable están unidos usando cable alargador, la distancia máxima de la estación es de 45 metros.

Ethernet: Utiliza una topología en bus lineal con método de acceso CSMA/CD (acceso múltiple por detección de portadora/detección de colisiones), usando cable coaxial fino o grueso, o par trenzado.

En estas redes cada paquete enviado por el cable es visible para todas las estaciones del segmento local, las estaciones comprueban la dirección del paquete, para determinar si están dirigidos a ellas; como todas las estaciones comparten el mismo cable, cualquier estación puede enviar un paquete, pero se produce una colisión cuando dos estaciones acceden simultáneamente al cable; cuando esto sucede ambas estaciones

esperan un tiempo aleatorio y reintentan la transmisión.

Estas colisiones causan pérdida en el rendimiento de la red, con más estaciones enviando paquetes el ancho de banda se satura; una solución consiste en dividir la red instalando otra placa de red en el servidor, otra utilizando un analizador de protocolos para saber si una estación está produciendo una cantidad excesiva de tráfico, o actuando en forma errática.

1.4 Cobertura de las redes:

Existen redes de diferentes tamaños, la red puede comenzar como algo pequeño y crecer con la organización.

- **Red de área local (LAN):** Es una red pequeña (de 3 a 50 nodos), localizada normalmente en un solo edificio o grupo de edificios pertenecientes a una organización como se aprecia en la figura 3.

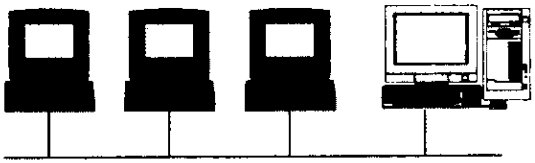

Figura 3. Red de área local (LAN).

- **Redes interconectadas (Internetwork):** Es una red de redes, se encuentra formada por dos o más segmentos de red local conectados entre sí, para formar un sistema que puede llegar a cubrir una empresa; esto es normal en empresas departamentalizadas, disponiendo cada departamento de su propia red local, estos interconectados entre sí; a menudo las redes más grandes se encuentran divididas en segmentos pequeños para optimizar el rendimiento y su gestión; para enlazar dos o más redes se utilizan ruteadores; una red de este tipo se muestra en la figura 4.
- **Red a nivel de empresa:** Una red a nivel de empresa es similar a una red interconectada, excepto que la red a nivel de empresa interconecta todos los sistemas informáticos de la organización, independientemente de los sistemas operativos que utilicen; en una red de este nivel se pueden conectar mini o grandes computadoras, estaciones de trabajo y cualquier otro elemento informático, en un único sistema interconectado.

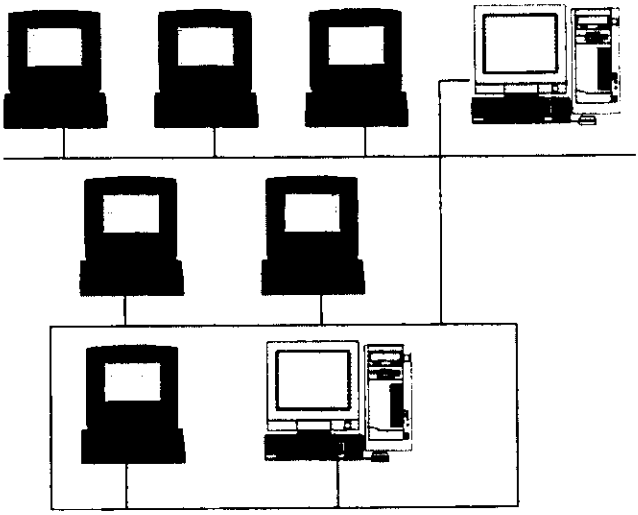

Figura 4. Interred (red de redes).

- **Red metropolitana (MAN) y red de gran alcance (WAN):** Estas redes ofrecen la conexión de redes y recursos distantes, las redes metropolitanas son normalmente redes de fibra óptica de gran velocidad que conectan segmentos de red local de un área específica, como un campus, un polígono industrial o una ciudad; estas redes utilizan unas líneas básicas de altas velocidad que conectan directamente los servidores, otra alternativa es la conexión con microondas dentro de la ciudad, las parábolas para microondas se montan en lo alto de los edificios apuntando de uno a otro para establecer la conexión entre las redes.

  La red metropolitana consta normalmente de un cableado y unos sistemas de comunicaciones que son instalados y propiedad del dueño de la red.

  Las redes de gran alcance permiten la interconexión nacional o mundial mediante las líneas telefónicas y satélites, las grandes empresas que poseen oficinas en grandes territorios por todo el mundo pueden interconectar sus redes de área local dentro de una red de gran alcance; los operadores de largas distancias alquilan líneas dedicadas para poder establecer la interconexión en forma dedicada y completa entre diversos sistemas; este tipo de conexiones son mucho más lentas que las conexiones vía redes locales, pero lo normal es que el tráfico también sea más reducido que el que hay en un segmento de red

local. Una red local transmite normalmente a unos 10Mb/seg y una de gran alcance lo hace a 1Mb/seg; esto está cambiando con la implantación de redes de fibra óptica a nivel nacional e internacional, con lo que se ofrece un mayor ancho de banda y una mayor velocidad de transferencia. Ejemplos de este tipo de red se muestra en la figura 5.

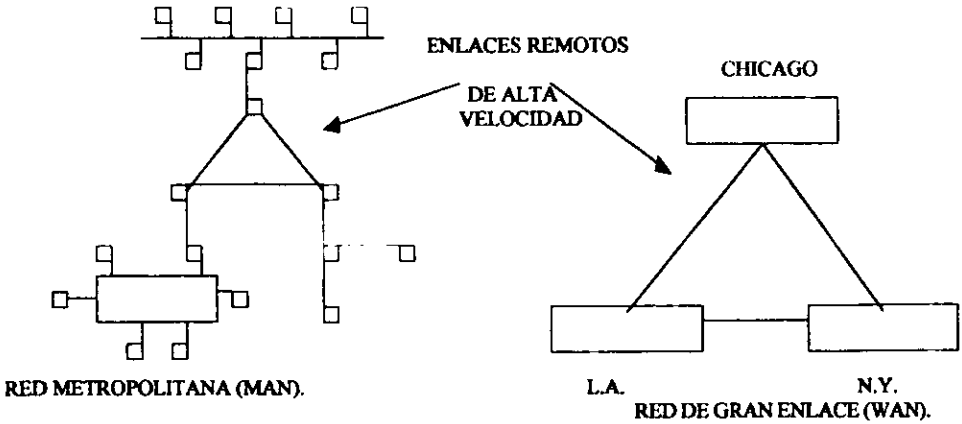

Figura 5. Redes MAN y WAN.

1.5 Beneficios de las RDC (Redes de Computadoras).

- **Compartición de programas y archivos:** Los programas y archivos de datos se pueden almacenar en un servidor de archivos, de forma que cualquier usuario en la red pueda acceder a ellos, los usuarios pueden almacenar sus archivos en directorios personales, o en directorios públicos, con lo que otros usuarios pueden leerlos o editarlos.
- **Compartición de los recursos de la red:** Entre los recursos de la red se encuentran las impresoras, trazadores, escáner y dispositivos de almacenamiento. En un sistema con servidor dedicado, los recursos se encuentran normalmente conectados al servidor de archivos, siendo compartidos por todos los usuarios, se pueden dedicar algunos servidores para imprimir (servidores de impresión) o commicarse (servidores de comunicación y correo).
- **Compartición de base de datos:** Un programa de base de datos es una aplicación ideal para una red, una de las características de la red denominada *bloqueo de registros* permite que varios usuarios

puedan acceder simultáneamente a un mismo archivo sin dañar la integridad de los datos; el bloqueo asegura que los usuarios no puedan editar a la vez un mismo registro.

- **Expansión económica de una base de PC:** Las redes ofrecen una forma económica de expandir la informatización en la organización, se pueden conectar estaciones de trabajo sin disco que utilicen la unidad de disco fijo del servidor para arrancar y almacenar sus archivos, de esta forma se ahorra en la compra de discos duros.
- **Posibilidad de utilizar software de red:** El software denominado software en grupo (*groupware*) está diseñado especialmente para redes, este permite a los usuarios interaccionar entre sí y coordinar sus actividades, es decir cada usuario puede compartir archivos o periféricos mediante una clave de acceso.
- **Uso del correo electrónico:** El correo electrónico permite comunicarse entre sí a los usuarios, los mensajes se dejan en unos buzones de los destinatarios para que sean accesados cuando lo desee el usuario.
- **Creación de grupos de trabajo:** Los grupos son importantes en la administración de la red, estos pueden estar compuestos por los usuarios que trabajan en un departamento o están asignados a un proyecto especial; se asignan usuarios a los grupos, y se dan acceso a directorios especiales y recursos que no serán accesibles a los restantes usuarios, de esta forma se evita tener que dar el derecho de acceso a cada uno de los usuarios de forma individual, también es más fácil dirigir mensajes y correo electrónico a grupos de usuarios.
- **Gestión centralizada:** Los servidores dedicados se pueden agrupar en un único lugar, las actualizaciones de hardware, las copias de seguridad del software y el mantenimiento y protección del sistema se pueden realizar de forma más sencilla si se encuentran en el mismo sitio.
- **Seguridad:** La seguridad comienza por el procedimiento de conexión al asegurar que un usuario accede a la red desde su propia cuenta de usuario, esta cuenta se crea específicamente de forma que le permite al usuario acceder sólo a las áreas autorizadas del servidor y de la red interconectada; las restricciones de conexión pueden forzar a un usuario a conectarse desde una estación de trabajo específica o sólo durante unos períodos de tiempo dados.

- **Mejoras en la organización de la empresa:** Las redes pueden modificar la estructura de una organización y la forma de gestionarse, los usuarios que trabajan en un departamento concreto para un responsable dado, no necesitan estar ahora en una misma localización física, sus oficinas pueden estar situadas en el lugar donde hagan más falta sus conocimientos, la red los une a sus responsables de departamento y compañeros; esta forma de organización es de especial interés en proyectos especiales, en los que personas de distintos departamentos, como los de investigación, producción y mercadeo, necesitan trabajar juntos.

CAPITULO 2

Estructura de una RDC.

2.1. Protocolos de comunicaciones:

Hace varios años parecía como si la mayor parte de los fabricantes de ordenadores y software fueran a seguir las especificaciones de la Organización Internacional para la Estandarización (ISO) sobre la Interconexión de Sistemas Abiertos (OSI); OSI define cómo los fabricantes pueden crear productos que funcionen con los productos de otros fabricantes sin la necesidad de controladores especiales o equipamiento opcional. El problema para implantar el modelo ISO/OSI fue que varias compañías ya habían desarrollado métodos para interconectar su hardware y software con otros sistemas.

Sin embargo, los estándares OSI ofrecen un modo útil para comparar la interconexión de redes y la interoperatividad entre varios vendedores, en este modelo hay varios niveles de protocolos en una jerarquía de protocolos, trabajando cada uno en diferentes niveles del hardware y del software.

2.1.1. Modelo OSI:

La figura 6, muestra el modelo OSI para interconexión, o jerarquía de protocolos; un *protocolo* es un modo definido de comunicación con otros sistemas.

- **Jerarquía de protocolos *OSI*:** Esta está definida por la ISO para promover una interoperatividad a nivel mundial; suele ser usada como estándar para comparar otras jerarquías de protocolos.

Nivel físico: Define las características físicas del sistema de cableado, abarca todos los métodos de red disponibles, incluyendo Token Ring, Ethernet y ArcNet, también define las comunicaciones por radio y por infrarrojos, fibra óptica y por cable RS-232-C para conectar módems a los ordenadores; este nivel especifica lo siguiente:

- Conexiones eléctricas y físicas.
- Cómo se convierte en un flujo de bits la información que ha sido empacada (metida en sobres o tramas) para ser transmitida por cable.
- Cómo consigue el acceso al cable la tarjeta de red.

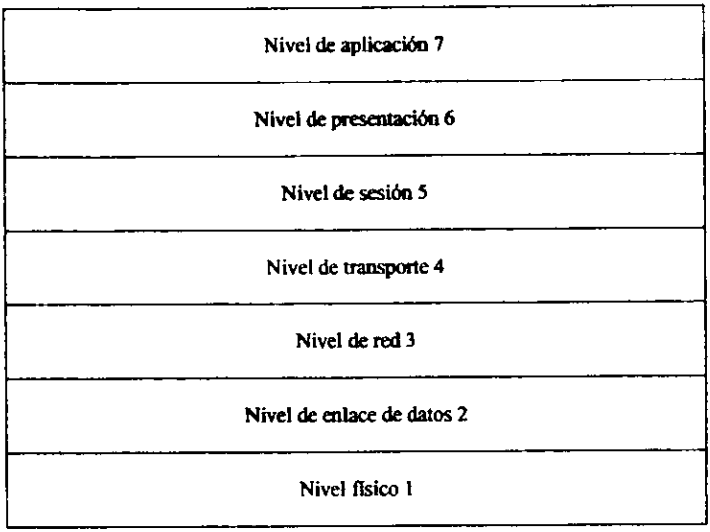

Figura 6. Jerarquía de protocolos OSI.

Nivel de enlace de datos: Define las reglas para enviar y recibir información a través de la conexión física entre dos sistemas; da por supuesto que el nivel físico ya ha establecido la conexión. Este nivel controla un flujo de datos empacados, si el flujo es muy rápido, la estación receptora deberá indicar que es necesaria una pausa para poder extraer la información; si un paquete llega defectuoso o no llega, se le indicará a la estación que envía los datos que los reenvíe.

Este nivel de enlace de datos se divide en dos subniveles: nivel MAC (Control de Acceso Medio), que se encarga de enviar los paquetes a sus destinos, y el nivel LLC (Control de Enlace Lógico), que recibe paquetes de niveles superiores y los envía al nivel MAC.

Los métodos de comunicación usados dependen del tipo de tarjeta de red que se use, se necesita instalar un controlador para la tarjeta con la jerarquía de protocolo adecuada para el tipo de comunicaciones que se va a manipular. En una misma red se debe usar el mismo tipo de tarjeta de red, para que exista compatibilidad.

Nivel de red: Define protocolos para abrir y mantener un camino entre equipos de la red, se ocupa del modo en que se mueven los paquetes, puede mirar la información sobre la dirección y determinar el mejor camino para transferir los datos a su destino. Si un paquete lleva la dirección de una estación en el mismo lugar, se envía la información directamente allí; si lleva dirección de otro segmento de la red, el paquete se envía a un dispositivo de enrutamiento (*Routing*), que elige el mejor camino a través de la red.

Es necesario usar dispositivos de enrutamiento cuando hay varias redes interconectadas para así optimizar la entrega de los paquetes.

Nivel de transporte: Suministra el mayor nivel de control en el proceso que mueve datos de un equipo a otro, este nivel proporciona un servicio de calidad y una entrega precisa encargándose de la detección de errores y su corrección; el nivel asigna un número de orden que es revisado en el receptor, si falta información del paquete al acabar la recepción, el protocolo acuerda un reenvío con el nivel de transporte del equipo transmisor.

Nivel de sesión: Este nivel coordina el intercambio de información entre equipos, se llama así por las sesiones de comunicaciones que establece y concluye; la coordinación es requerida cuando un equipo es más lento que otro o si la transferencia de paquetes no está ordenada, añade al paquete información sobre el protocolo de comunicaciones que se debe usar, y mantiene la sesión hasta que finaliza la transferencia de información.

Nivel de presentación: En este nivel, los protocolos son parte del sistema operativo y de la aplicación que el usuario acciona en la red, la información es formateada para aparecer en pantalla o ser impresa, los códigos incluidos en la información son interpretados como etiquetas o secuencias gráficas especiales; este nivel también maneja el cifrado de los datos y la manipulación de otros conjuntos de caracteres.

Nivel de aplicación: En este nivel, el sistema operativo de red y sus aplicaciones se hacen disponibles a los usuarios, estos emiten órdenes para requerir los servicios de red, y esas órdenes son empacadas y enviadas a través de los diferentes niveles más bajos del protocolo.

2.1.2. Protocolo de Novell *SPX/IPX*:

El protocolo NetWare Secuencia de Intercambio de Paquete/Intercambio de Paquete en red Interna (SPX/IPX) es el protocolo nativo usado por Novell NetWare, derivado de la jerarquía de protocolos de Servicios de Red Xerox (Xerox Network Services, XNS). El IPX es un protocolo de enrutamiento, y los paquetes IPX contienen direcciones de red y de estación; está información va en el paquete en forma de datos de cabecera. El SPX es una versión mejorada del IPX; es una interfaz de programación utilizada por desarrolladores de software para crear aplicaciones que requieran un intercambio de paquetes garantizado entre programas, el SPX ofrece un método para confirmar la recepción de un paquete.

2.1.3. Protocolo de Microsoft *NetBeui*:

Este protocolo, es un protocolo no direccionable, esto es el ordenador no requiere una dirección de red, sólo un nombre de PC, y actúa únicamente en redes LAN. Para poder accesar a los archivos o periféricos de otras máquinas, es necesario que estas tengan dichos recursos como compartidos; la conexión se hace indicando sólo el nombre de la máquina y/o recurso al que se desea accesar. No precisa de una configuración compleja.

2.1.4. Protocolo *TCP/IP*:

Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) fue una de las primeras jerarquías de protocolos, originalmente fue puesto en práctica por el Departamento de Defensa como un modo de unir los productos de red de varios fabricantes; la parte IP proporciona actualmente una de las mejores definiciones para la interconexión de redes. Este protocolo sé vera más a detalle más adelante.

2.1.5. Protocolo NFS:

El Sistema de Archivos de Red (NFS) es un sistema de archivos para entornos UNIX. NFS es un sistema de archivos distribuido que está construido sobre TCP/IP, permite a los usuarios acceder a archivos de sistemas remotos como si estos formaran parte de su propio sistema; no se requieren órdenes o procedimientos adicionales para listar archivos o ver su contenido, el sistema de archivos remoto es asignado como una unidad local.

2.1.6. Protocolo FRAME RELAY:

Frame Relay es un protocolo de transmisión de paquetes de datos, en ráfagas de alta velocidad a través de una red digital fragmentados en unidades de transmisión llamadas Frame. Frame Relay requiere de una conexión exclusiva durante el periodo de transmisión; esto no es válido para transmisiones de video y audio ya que requieren un flujo constante de transmisiones.

Frame Relay es una tecnología de paquete-rápido ya que el chequeo de errores no ocurre en ningún nodo de transmisión; los extremos son los responsables del chequeo de errores.

Un paquete rápido es transferido en modo asíncrono (ATM) con cada Frame Relay o elemento de transmisión, Frame Relay transmite paquetes en el nivel de envío de datos del modelo OSI entes que en el nivel de red. Distinto a un paquete que es de tamaño fijo, un Frame es variable en tamaño y pude ser tan largo como mil bytes o más.

2.2. Interconexión de redes:

Interconexión e interoperatividad son palabras que se refieren a la consecución de que equipos y aplicaciones de distintos fabricantes trabajen conjuntamente en una red, pero en una empresa grande, se dan varias situaciones:

- Hay varias LAN instaladas por separado en diferentes departamentos, usando posiblemente distintos tipos de medio.
- Los usuarios quieren conectarse a un equipo anfitrión desde sus equipos.
- Hay una multitud de sistemas en uso, incluyendo equipos basados en DOS, Macintosh, equipos SUN (servidores UNIX con NFS), minicomputadoras y grandes computadoras.

La interoperatividad entra en juego cuando es necesario repartir archivos entre ordenadores con sistemas operativos diferentes, o para controlar todos esos equipos distintos desde una consola central; también se debe hacer que los protocolos permitan comunicarse al equipo con cualquier otro. Varias redes que usen distintos protocolos no pueden comunicarse, por ejemplo una aplicación de un equipo que usa SPX/IPX no puede comunicarse directamente con un equipo que utiliza TCP/IP, sin embargo las compuertas (pasarelas) convierten cada nivel de los protocolos, de modo que el equipo de un usuario puede acceder al sistema operativo de un equipo huésped que use un protocolo diferente.

El nivel de protocolo para redes e interconexión de redes incluye los niveles de red y de transporte; define la conexión de redes similares y enrutamiento entre redes similares o distintas, en este nivel se da la interconexión entre topologías distintas, pero no la interoperatividad; en este nivel es posible *filtrar* paquetes sobre una LAN en una interconexión de redes, de manera que no necesiten saltar a otra LAN cuando no es necesario.

A continuación, la figura 7 ilustra los distintos tipos de conexiones posibles (usando repetidores, puentes y ruteadores).

2.3. Repetidores:

Un repetidor amplifica la señal en un cable de la red haciendo posible una ampliación de la extensión del cable y de la red, no requiere software, y normalmente es un aparato autónomo que no añade información a la transmisión de datos; una vez conectado, un repetidor transmite la información de forma transparente y sin retardo.

A medida que las señales eléctricas se transmiten por un cable, tienden a degenerar proporcionalmente a la longitud del cable, esto se conoce como ***atenuación***, se instala entonces un repetidor para amplificar la señal del cable, de modo que se pueda extender la longitud de la red; el repetidor normalmente no modifica la señal, excepto en que la amplifica para poder retransmitirla por el segmento de cable extendido, algunos repetidores también filtran el ruido. Estos tiene las siguientes características:

- Regenera las señales de la red para que lleguen más lejos.
- Se utilizan sobre todo en los sistemas de cableado lineales como Ethernet.
- Funcionan sobre el nivel más bajo de la jerarquía de protocolos: el nivel físico.
- Los segmentos conectados deben utilizar el mismo método de acceso al medio de transmisión.
- Se utilizan normalmente dentro de un mismo edificio.
- Los segmentos conectados con un repetidor forman parte de la misma red, y tendrán la misma dirección de red.

Los repetidores funcionan normalmente a la misma velocidad de transmisión que las redes que conectan; dada en paquetes por segundo (pps), está se encuentra alrededor de 15,000 pps para una red Ethernet típica.

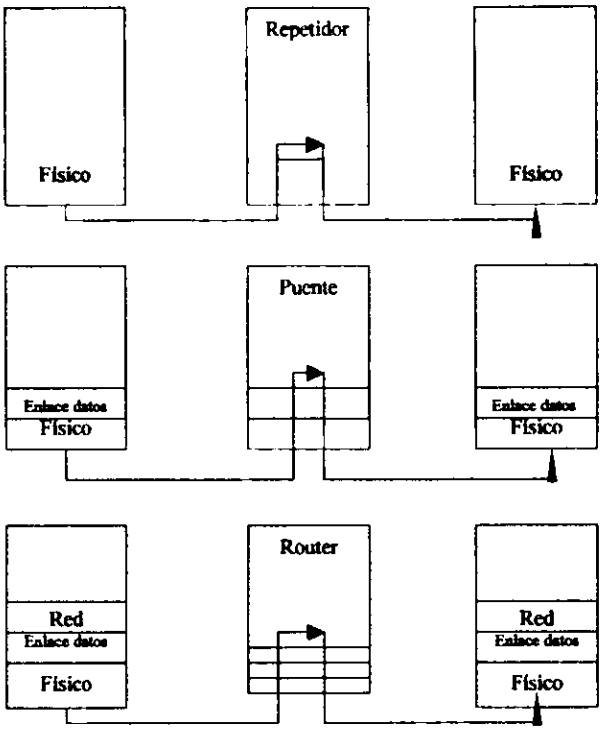

Figura 7. Repetidores, puentes y routers.

Puentes:

Este es un dispositivo del nivel de enlace de datos que interconecta dos redes que tengan o no la misma topología; se puede crear un puente en un servidor NetWare añadiéndole simplemente dos tarjetas de red por ejemplo, añadiendo al servidor las tarjetas Ethernet y Token Ring, los usuarios de cada segmento de la red se pueden comunicar entre sí. Un puente utiliza el nivel de Control de Acceso al Medio (MAC), que es la mitad inferior del nivel de enlace de datos, este nivel contiene la dirección de la estación de destino, como el puente puede ver todos los equipos de todas las LAN interconectadas, simplemente remite el paquete al equipo correcto; el tráfico entre LAN no es filtrado como cuando es controlado por un ruteador, así que se pueden producir algunas pérdidas de rendimiento en situaciones con altas cargas de tráfico.

Un puente añade un nivel de inteligencia a una conexión entre redes, conecta dos segmentos de red iguales o distintos; podemos ver un puente como un clasificador de correo que mira las direcciones de los paquetes y los coloca en la red adecuada. Cada segmento de red puede ser de un tipo distinto (Ethernet, Token Ring, ArcNet etc.). Se puede crear un puente para dividir una red amplia en dos o más redes pequeñas, esto mejora el rendimiento al reducir el tráfico, ya que los paquetes para estaciones concretas no tienen que viajar por toda la red; los puentes trabajan en el nivel de enlace de datos, cualquier dispositivo que se adapte a las especificaciones del nivel de control de acceso al medio (MAC) puede conectarse con otros dispositivos del nivel MAC. Con un puente se pueden conectar dispositivos que utilicen protocolos diferentes, pero el nivel de enlace de datos no sabe nada sobre el mejor camino hacia un cierto destino; no existe ninguna forma de enviar paquetes a un segmento de red de modo que alcancen su destino de la forma más rápida o eficiente; no obstante, los puentes ofrecen filtrado, el filtrado evita que los paquetes de un segmento de red local pasen por el puente y lleguen a segmentos de red donde no sirven para nada. Esto ayuda a reducir el tráfico entre redes e incrementa el rendimiento; sin filtrado los paquetes son enviados a todos los puntos de la red.

Se instala un puente por lo siguiente:

- Para extender una red existente cuando se ha alcanzado su máxima extensión.
- Para eliminar los cuellos de botella que se generan cuando hay demasiadas estaciones de trabajo conectadas a un único segmento de red, de esta forma cada red trabaja con menos usuarios, mejorando el rendimiento.
- Para conectar entre sí distintos tipos de redes, como Token Ring y Ethernet.

Cuando se establece un puente, cada segmento de red posee una dirección de red distinta, esta dirección se puede considerar como una calle, y cada estación de trabajo como una casa en dicha calle. La dirección de un segmento de red se asigna al instalar la red, se utiliza para encaminar los paquetes entre redes.

2.4. Tipos de puentes:

2.4.1. Puentes con aprendizaje:

Los puentes con aprendizaje, o adaptativos, se "aprenden" las direcciones de las otras estaciones de la red, por lo que no es necesario que el instalador del puente cree una tabla con las direcciones en el puente. Las estaciones difunden continuamente sus señales de identificación, y los puentes pueden construir sus tablas a partir de estas direcciones. En la actualidad, la mayor parte de los puentes poseen aprendizaje.

2.4.2. Puentes en tándem:

Cuando una conexión con un puente es crítica, puede ser necesario crear puentes redundantes tolerantes a fallos, si un puente falla, el otro puede continuar con el tráfico; sin embargo, cuando hay dos enlaces, existe la posibilidad de que el tráfico pase por uno y vuelva por el otro de nuevo, creándose un esquema circular de movimiento de paquetes que continuaría sin fin. Los puentes en tándem detectan y rompen los bucles anulando ciertas conexiones.

2.4.3. Puentes con distribución de carga:

El puente con distribución de carga es la forma más eficiente de puente, utiliza un algoritmo de emparejamiento, pero también utiliza una conexión doble para transferir los paquetes, mejorando de esta forma el rendimiento global de la red.

2.5. Ruteadores (Routers):

Un ruteador opera un peldaño más arriba que un puente en la escalera de protocolos; los ruteadores interconectan segmentos de la red a través del nivel de la red. Un ruteador se diferencia de un puente en la medida en que es capaz de leer de un paquete tanto la dirección del equipo de destino como de la LAN, por ello los ruteadores pueden filtrar paquetes y dirigirlos a un equipo utilizando la mejor ruta posible.

Los ruteadores son críticos para las redes de gran enlace que utilizan enlaces de comunicaciones remotas, mantienen el tráfico fluyendo eficientemente sobre caminos predefinidos en una interconexión de redes compleja; las grandes redes que se extienden por todo el mundo pueden contener muchas conexiones remotas redundantes, en ese caso resulta importante encontrar el mejor camino entre el origen y el destino. Este es el origen de los ruteadores, pueden inspeccionar la información en el nivel de red para determinar la información de la mejor ruta. Las razones para usar ruteadores en lugar de puentes son:

- Los ruteadores ofrecen un filtrado de paquetes avanzado.
- Los ruteadores son necesarios cuando hay diversos protocolos en una interconexión de redes, y los paquetes de ciertos protocolos tienen que confinarse en una cierta área.
- Los ruteadores ofrecen un encaminamiento inteligente, lo cual mejora el rendimiento. Un ruteador inteligente conoce la estructura de la red y puede encontrar con facilidad el mejor camino para un paquete.

- Como los ruteadores realizan un filtro avanzado, son importantes cuando se utilizan líneas de comunicación remota lentas y caras.

Funcionamiento del ruteador.

Un ruteador examina la información de encaminamiento de los paquetes y los dirige al segmento de red adecuado, si el ruteador está en un servidor, envía los paquetes destinados para ese servidor a los protocolos de niveles superiores; un ruteador sólo procesa los paquetes que van dirigidos a él, lo que incluye a los paquetes enviados a otros ruteador con los que esté conectado; los ruteadores envían los paquetes por la mejor ruta hacia su destino, mantienen tablas de redes locales y ruteos adyacentes en la red, cuando un ruteador recibe un paquete, consulta estas tablas para ver si puede enviar directamente el paquete a su destino, si no es así, determina la posición de otro ruteador que pueda enviar el paquete a su destino.

Los ruteadores pueden ser específicos para un protocolo o pueden manejar diversos protocolos. Los ruteadores permiten dividir una red en redes lógicas, estas redes lógicas son más sencillas de manejar, cada segmento de red tiene su propio número de red local, y cada estación de dicho segmento tiene su propia dirección, esta es la información contenida en el nivel de red al que acceden los ruteadores. La segmentación de las redes permite evitar *las tormentas de difusión*, estas ocurren cuando los nodos no se conectan de forma adecuada, y la red se satura con la difusión de mensajes intentando localizar los destinos; los métodos de filtrado y selección del mejor camino utilizado, al segmentar ayudan a reducir este efecto.

2.6.Pasarelas (Gateways):

Los pasarelas permiten interconectar sistemas con distintos protocolos, estos pasarelas convierten cada nivel de los protocolos de modo que el equipo de un usuario puede acceder al sistema operativo de un equipo huésped que utilice un protocolo diferente. Funcionan en los niveles más altos de la jerarquía de protocolos, permitiendo la interconexión de sistemas y redes que utilizan protocolos incompatibles. Esto se muestra en la figura 8.

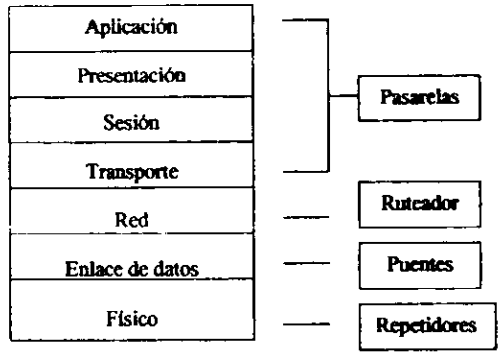

Figura 8. Niveles de protocolos OSI utilizados por los dispositivos de interconexión de redes.

CAPITULO 3

Redes TCP/IP.

3.1. Protocolo TCP:

El Protocolo de Control de Transmisión (la parte TCP de TCP/IP), es un protocolo de comunicaciones, que proporciona transferencia confiable de datos. Es responsable de ensamblar datos pasados desde aplicaciones de capas superiores a paquetes estándar y asegurarse que los datos se transfieran correctamente. TCP/IP se hizo importante cuando el departamento de defensa de los Estados Unidos empezó a incluir los protocolos como estándares militares, lo cual era necesario para muchos contratos; se volvió popular principalmente por el trabajo que se realizó en UCB (Berkley), UCB fue un centro de desarrollo de UNIX, en 1983 emitieron una versión que incorporaba a TCP/IP como elemento integral, esta versión quedó disponible como software de dominio público.

3.2. Protocolo IP:

El Protocolo Internet (Internet Protocol, IP) es responsable de mover a través de las redes los paquetes de datos ensamblados, ya sea por TCP o Protocolo de Datagrama de Usuario UPD (User Datagram Protocol), a fin de determinar enrutamientos y destinos, utiliza un conjunto de direcciones únicas para cada dispositivo de red. Este protocolo asegura la conectividad universal del sistema.

3.3. OSI y TCP/IP:

La adopción de TCP/IP no entraba en conflicto con los estándares OSI, porque ambos se desarrollaron en forma simultánea, sin embargo hay varias diferencias, que se originan en los requerimientos básicos de TCP/IP; las diferencias están relacionadas con las capas encima del nivel de transporte, y las que corresponden al nivel de red, OSI tiene tanto una capa de sesión como una capa de presentación, en tanto que TCP/IP combina ambas en una capa de aplicación; el requisito de un protocolo sin conexión también hacía que TCP/IP combinara las capas física y de vínculo de datos de OSI en el nivel de red. TCP/IP denomina a los distintos elementos de niveles de red como subredes. Estas estructuras se presentan en la figura 9.

La combinación de las capas de vínculo de datos y la física en una sola permitía que se diseñara una subred que resultara independiente de muchos protocolos de red, porque TCP/IP es ajeno a los detalles, esto permite a las redes propietarias, autónomas implementar protocolos TCP/IP para conectividad por fuera de sus sistemas cerrados.

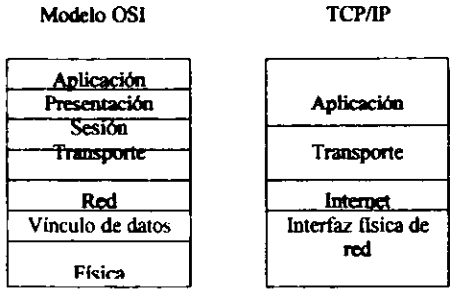

Figura 9. Las estructuras en capas OSI y TCP/IP.

3.4. Dirección IP:

La dirección de Protocolo Internet (IP) de un nodo es su dirección lógica, independiente de su dirección física asignada a la tarjeta de red por su fabricante, la dirección IP también es independiente de la configuración de la red, estas direcciones tienen siempre el mismo formato, independientes del tipo de red que se utilice. El formato es de 4 bytes (32 bits) que identifica tanto una red como un sistema local o nodo de la red, cada dirección debe ser única, constando de cuatro números decimales separados por puntos, por ejemplo **119.141.254.190.** En cada tipo de red, el protocolo TCP/IP asigna la dirección IP a la dirección de nodo física para su entrega, los paquetes (datagramas) contienen la dirección IP del remitente, por lo que las estaciones receptoras pueden responder si es necesario. La dirección IP identifica la red y el nodo de la red en que se encuentra el remitente.

La dirección de cuatro bytes IP se encuentra dividida en una parte de red que identifica la red y en una parte de sistema (hosts) que identifica la computadora (nodo), la porción de red debe ser la misma para todos los nodos de la red. Hay cuatro esquemas de asignación de dirección:

- Los esquemas de direccionamiento de Clase "A", en que el primer byte es la dirección de la red y los tres últimos la dirección del nodo. Esto permite hasta 126 redes con 16 millones de nodos de red.
- Los esquemas de direccionamiento Clase "B", en que los dos primeros bytes constituyen la dirección de red y los dos últimos la dirección del nodo. Esto permite 16,000 redes y 65,000 nodos.
- En los esquemas de direccionamiento Clase "C", los tres primeros bytes representan la dirección de red y el último la dirección de nodo, con lo que se permiten hasta 2 millones de redes con 254 nodos cada una.

- Existe un esquema Clase "D", se usan con fines de multidifusión, cuando se requiere una difusión general a más de un dispositivo.

3.4.1. Direccionamiento en subredes:

En una red son necesarias varias porciones de la información para asegurar la entrega correcta de datos, los componentes son, la dirección física y la dirección de vínculo de datos:

Direcciones físicas: Cada dispositivo de una red que se comunica con otros tiene una *dirección física única* también conocida como dirección de hardware; para el hardware, las direcciones están cifradas en tarjetas de red, establecidas mediante interruptores o software. En la capa física se realiza el análisis de cada datagrama que se recibe, si la dirección del receptor coincide con la dirección física del dispositivo, el datagrama puede pasar hacia arriba por las diferentes capas, si no coinciden las direcciones, se ignora el datagrama.

Dirección de vínculo de datos: Los estándares Ethernet utilizan una dirección que se conoce como dirección de la capa de vínculo (LSAP), está sirve para verificar el tipo de protocolo de vínculo que se utiliza en la capa de vínculo de datos: igual que en las direcciones físicas, un datagrama contendrá tanto LSAP del emisor como del receptor.

3.5. Protocolos de ruteo:

3.5.1 ARP:

La determinación de las direcciones puede resultar difícil porque puede ser que no todas las máquinas de la red tengan la lista de todas las direcciones de las demás máquinas o dispositivos, el envío de datos de una máquina a otra puede causar problemas si no se conoce la dirección física de la máquina receptora, y si no existe un sistema de resolución (conversión) para determinar las direcciones; tener que utilizar en forma constante una tabla de direcciones en cada una de las máquinas podría resultar laborioso. El problema no se restringe a direcciones de máquina de una red pequeña, porque si se desconocen las direcciones de la red de destino remoto, también ocurrirán problemas de enrutamiento y entrega. Es por esto que se requiere de protocolos de ruteo; estos protocolos se encargan de comunicar dos o más ruteadores que manejen diferente protocolo, es decir convierten los protocolos para que se de la correcta comunicación entre dos máquinas que se encuentran en dos lugares muy distantes (diferente edificio).

El Protocolo de Resolución de Direcciones (ARP) ayuda a resolver estos problemas, la tarea del ARP es convertir las direcciones IP a direcciones físicas (de red y local MAC), y al hacerlo elimina la necesidad de

que las aplicaciones sepan direcciones físicas; esencialmente el ARP es una tabla con una lista de direcciones IP y sus direcciones físicas correspondientes, la tabla se conoce como *caché ARP*.

Cuando ARP recibe la dirección IP de un dispositivo receptor, busca en el caché ARP alguna coincidencia, si encuentra alguna, devuelve la dirección física; si no es así envía un mensaje a la red. El mensaje conocido como *solicitud ARP*, es una difusión que se recibe en todos los dispositivos de la red local; la solicitud contiene la dirección IP del dispositivo receptor deseado, si un dispositivo reconoce la dirección IP como suya, envía un mensaje de respuesta con la dirección física de regreso a la máquina que generó la solicitud ARP, y ésta coloca la información en su caché ARP para su uso futuro. Siempre que se recibe una solicitud el caché ARP utiliza la información incluida en la solicitud para actualizar su propia tabla, por lo que el sistema se adecua en forma dinámica a direcciones físicas cambiantes y a nuevas adiciones a la red, sin tener que generar una solicitud ARP propia.

3.5.2. OSPF:

El protocolo OSPF se desarrolló con la esperanza de que resultara el protocolo dominante dentro de Internet, una buena descripción del sistema es "ruta óptima". OSPF utiliza la información de dirección de destino y de tipo de servicio (TOS) en un encabezado de datagrama IP a fin de desarrollar la ruta, a partir de una tabla de enrutamiento que contiene información sobre la topología de la red, una compuerta OSPF determinará la ruta más corta utilizando métrica de costos, cual factor en velocidad de ruta, tráfico, confiabilidad y seguridad. Siempre que las comunicaciones deben salir de una red autónoma, OSPF llama a este enrutamiento externo de los cuales existen dos: una ruta de tipo 1 incluye los mismos cálculos para la ruta externa que para la interna (se aplican los mismos algoritmos), una ruta de tipo 2 utiliza sólo el sistema OSPF para calcular una ruta a la compuerta del sistema destino, ignorando cualquier otra ruta del sistema autónomo remoto, esto tiene como ventaja el hecho de que resulta independiente del protocolo en la red destino y elimina la necesidad de convertir los parámetros allí incluidos.

OSPF permite que una red autónoma grande se divida en áreas más pequeñas, cada una con su propia compuerta y algoritmos de enrutamiento. En OSPF se utilizan dos formatos de encabezado, el formato aparece en la figura 10.

3.5.3. RIP:

El Protocolo de Información de Enrutamiento (RIP) utiliza una tecnología de difusión, esto significa que a intervalos regulares las compuertas difunden sus tablas de enrutamiento a otras compuertas de red; RIP tiende a obtener información sobre todos los destinos en el sistema autónomo al cual pertenecen las compuertas, RIP es un sistema vector-distancia, enviando en sus mensajes la dirección de red y la distancia a la dirección.

Una máquina en una red basada en RIP puede estar activa o pasiva, si está activa, envía sus tablas de enrutamiento a las demás máquinas; la mayor parte de las compuertas son dispositivos activos, una máquina pasiva no envía sus tablas de enrutamiento, pero puede enviar o recibir mensajes que sí afecten a su propia tabla de enrutamiento; la mayor parte de las máquinas orientadas a usuario (PCs y estaciones de trabajo) son dispositivos pasivos. El formato de los mensajes RIP aparece en la figura 11.

Versión (8 bits)
Tipo (8 bits)
Longitud del paquete (16 bits)
Identificador del ruteador (32 bits)
Identificación del área (32 bits)
Suma de verificación (16 bits)
Tipo de autentificación (16 bits)
Autentificación (64 bits)

Figura 10. Formato de encabezado de mensaje OSPF.

Un mensaje de solicitud se envía a otra compuerta cuando se requiere una actualización de enrutamiento; cuando se recibe una solicitud, el sistema examina el mensaje para verificar cada una de las direcciones de red incluidas, si su tabla tiene una distancia a esa dirección de red, en la respuesta se coloca en el campo correspondiente métrico.

Cada máquina basada en RIP en la red mantiene una tabla de enrutamiento, con una entrada para cada máquina con la cual se puede comunicar.

Valor de comando
Número de versión
Reservado

Familia
Dirección de red
Dirección de red
Dirección de red
Métrica (distancia)

Figura 11. Formato de mensaje RIP.

Un sistema de administración permite a los supervisores ver y gestionar todos los recursos de la red, independientemente del hardware o sistema operativo que utilicen; a medida que las interconexiones de redes se expanden, los administradores necesitan un método para gestionar los recursos remotos sin tener que desplazarse físicamente hasta ellos. Los sistemas de administración ofrecen una forma de recoger información de varios sistemas en ubicaciones distintas y mostrarla en un sistema central, en el que los administradores pueden manipularla e interpretarla, SNMP es un estándar para recoger información de red que nació a partir de Internet; SNMP tiene agentes que recogen información de los dispositivos de la red y la envían a una base de información de gestión, las aplicaciones compatibles con SNMP pueden utilizar esta información para dar el estado de la red y otra información a los administradores del sistema.

3.6. Internet:

Este término se refiere a la red colectiva de todas las subredes, lo que tienen en común es que utilizan TCP/IP como protocolo de comunicaciones; la organización de Internet y la adopción de nuevos estándares están controlados por el Consejo Consultivo Internet (IAB). Debido a que el gobierno de los Estados Unidos fue el responsable del financiamiento del desarrollo de Internet, conserva gran parte del control y del patrocinio de la investigación y la expansión de Internet.

Las distintas redes conectadas entre sí a través de enrutadores se conocen como subredes, debido a que forman una pequeña parte de la red general más grande, con TCP/IP todas las interconexiones entre redes

físicas se hace mediante compuertas (enrutadores); un punto importante es que, las compuertas enrutan los paquetes de información basados en su nombre de red de destino, y no en la máquina destino.

Internet está formado por cuatro capas, esta arquitectura se muestra en la figura 12, estas capas no deben confundirse con la arquitectura de cada máquina, sino como un método para apreciar cómo funcionan juntos la interred, la red local, TCP/IP y cada máquina individual, las máquinas independientes residen en la capa de subred en la parte inferior de la arquitectura, conectadas juntas en una red de área local LAN e identificadas como la subred, por encima de la capa de subred está la interred, que proporciona la funcionalidad para las comunicaciones entre redes a través de compuertas, cada subred utiliza compuertas para conectarse a otras subredes en la interred, en esta capa los datos son transferidos de una compuerta a otra hasta que llegan a su destino, y entonces pasan a la capa de subred. El Protocolo Internet (IP) corre en la capa de Interred.

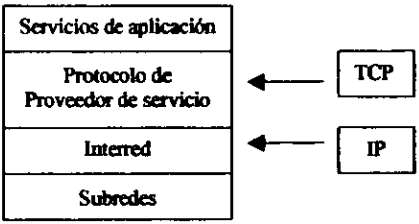

Figura 12. La arquitectura Internet.

La capa del protocolo de proveedor de servicios es responsable de las comunicaciones de extremo a extremo de la red, esta es la capa donde corre el Protocolo de Control de Transmisión (TCP), por sí misma maneja el flujo de tráfico datos y asegura la confiabilidad de la transferencia del mensaje.

La capa más alta es la de los servicios de aplicación, que soporta las interfaces con las aplicaciones de usuario; esta capa es la interfaz para el correo electrónico, las transferencias remotas de archivos y el acceso remoto.

3.6.1. Sistema de Nombre de Dominio (DNS):

Las direcciones de red son análogas a las direcciones de correos, en el sentido de que le indican a un sistema dónde debe entregar un datagrama. Tres términos utilizados comúnmente en Internet se relacionan con el direccionamiento: nombre, dirección y ruta.

El **nombre** es una identificación específica de una máquina, un usuario o una aplicación, por lo general es único y proporciona un objetivo absoluto para el datagrama, una **dirección** típicamente identifica la

localización del objetivo, (su localización física o lógica) en una red; una **ruta** le dice al sistema como hacer llegar el datagrama a la dirección correcta.

Un paquete de software de red, conocido como **servidor de nombres**, tratará de descifrar la dirección y la ruta a partir del nombre, realizándolo de forma transparente para el usuario; cuando se envía correo electrónico, sólo se da el nombre del destinatario, apoyándose en el servidor de nombres para que haga entrega del mensaje de correo.

En vez de utilizar la dirección IP completa, muchos sistemas adoptan nombres más significativos para sus dispositivos y redes, por lo general los nombres de las redes reflejan el nombre de la organización como por ejemplo **nissan.com**; los nombres individuales de los dispositivos de la red pueden ir desde nombres descriptivos en redes pequeñas como **laser_1**; a convenciones de asignación de nombres más complejos en redes más grandes. La conversión entre estos nombres y las direcciones IP sería prácticamente imposible a escala total de Internet.

A fin de resolver el problema de los nombres de red, el Centro de Información de Red (NIC) mantiene una lista de los nombres de red y de las direcciones correspondientes de las compuertas de red, este sistema creció de una sencilla lista de archivo plano (en la cual se buscaban coincidencias), a un sistema más complejo conocido como Sistema de Nombre de Dominio (DNS), cuando las redes se hicieron demasiado numerosas para que el sistema de archivo plano funcionara eficazmente.

El DNS utiliza una arquitectura jerárquica, parecida al sistema de archivo de UNIX, el primer nivel de asignación de nombre divide las redes en categorías de subredes, como **com** para comercial, **mil** para militar, **edu** para educativo, etc. Por debajo de cada una de éstas se encuentra otra división, que identifica a la subred individual, por lo general una para cada organización, esta se conoce como ***nombre de dominio*** y es única; el administrador de sistemas de la organización puede dividir aún más las subredes de la empresa según desee, con cada red identificada como *subdominio*, por ejemplo el sistema **merlin.abc_corp.com** tiene como nombre de dominio abc_corp.com, en tanto que la red merlin.abc_corp es un subdominio de merlin.abc_corp.com; una red se puede identificar mediante ***un nombre absoluto*** (merlin.abc_corp.com) o un ***nombre relativo*** (merlin) que utiliza sólo parte del nombre completo del dominio.

Se han establecido seis nombres de dominio de primer nivel:

.arpa Una identificación ARPAnet-Internet

.com Empresa comercial

.edu Institución educativa

.gov Cualquier organización de gobierno

.mil Militar

.org Cualquier otra que no caiga dentro de las categorías anteriores

El NIC permite agregar un indicador de país como **ca** para Canadá, **mx** para México, etc. El DNS utiliza dos sistemas para establecer y controlar los nombres de dominio, en cada red un *resolvedor de nombres* examina la información incluida en un nombre de dominio, si no puede determinar la dirección IP completa, consulta a un *servidor de nombres* que tiene disponible toda la información del NIC, este resolvedor trata de completar la información de direccionamiento mediante su propia base de datos, la cual actualiza cuando consulta a un servidor de nombres; si el servidor de nombres no puede convertir la dirección, consulta a otro servidor y así sucesivamente a través de toda la interred.

CAPITULO 4.

Consideraciones para el diseño de una red:

En el presente capítulo se vera el diseño de una red LAN, la forma en que el protocolo TCP/IP es utilizado para la optimización de los recursos y su comunicación con el exterior (redes LAN, WAN; etc.), problemas y su solución.

4.1. Identificación de las necesidades:

Se debe preparar un plan de forma profesional para implementar una red. La tecnología y las necesidades personales de los usuarios cambian constantemente, por ello debe desarrollarse dicho plan con las consultas al personal que de esta forma ayudara a identificar los problemas y las necesidades tales como:

- La eficiencia del sistema actual, tanto si es manual como si está sistematizado.
- Si los sistemas existentes disponen de una capacidad de almacenamiento suficiente, para las necesidades actuales.
- Es necesario ejecutar un programa multiusuario o una base de datos centralizada que requiere de una red local.
- Los usuarios requieren utilizar los periféricos que se encuentran conectados a otros equipos.
- Los usuarios necesitan de una forma de comunicación más eficiente, pudiendo ser el correo electrónico la mejor solución.
- Se requiere obtener u ofrecer información a otras fuentes ajenas a la institución, y esto puede realizarse a través de Internet.

Cualquiera que intente identificar las necesidades a cubrir por una red tendrá que estar familiarizado con el equipo que se está utilizando en ese momento y sus limitaciones.

Identificación y evaluación del equipo existente. Se requiere toda la información posible sobre los equipos que se están utilizando en la empresa, como los tipos de PC y sus dispositivos de almacenamiento, sistemas de copia de seguridad, impresoras, trazadores gráficos y equipo de comunicaciones, además de otros equipos que se encuentren en lugares remotos.

Representación del posible entorno de la red. Se debe dibujar un plano arquitectónico completo del lugar de la instalación, incluyendo la ubicación de los equipos, y periféricos definidos anteriormente; se deben localizar las tomas de red, cableado, racks, concentradores, ruteadores y/o modems.

Evaluación del uso. Se debe tratar de determinar el número de usuarios que accederán a la red, y los requisitos del servidor de archivos y disco de los usuarios; si se tienen varios departamentos se deberá tomar en cuenta si cada uno de estos debe disponer de su propio segmento de red conectado a los otros, ¿cuánto espacio necesitará cada departamento en los servidores?, ¿cada departamento tendrá su propio servidor?, ¿éste, será administrado por el propio departamento, o se gestionarán desde un lugar centralizado?.

Determinación de interdependencias. Se deben identificar si existen interdependencias entre los usuarios de los diferentes departamentos, de forma que se puedan conectar físicamente a través de la red, dándoles ciertos derechos de acceso a los diferentes recursos.

4.2. Evaluación de las necesidades de equipo y rendimiento:

El rendimiento de nuestra red va a estar determinado por el tipo de cableado (ancho de banda), tipo de tarjeta de red (si maneja 8, 16 ó 32 bits de datos), el software de red, etc. actualmente un servidor posee 32Mb de memoria RAM, como mínimo (puede haber servidores de 128 Mb en RAM) y discos que van desde 2.1Gb hasta 12Gb de almacenamiento. La velocidad a la que la red trata los momentos de tráfico más denso se denomina ***rendimiento general***, este depende de diferentes elementos, incluyendo el cableado, la velocidad del servidor y la velocidad de las estaciones de trabajo, un cuello de botella en el servidor afecta al rendimiento general de toda la red, por ello es necesario adquirir equipos que puedan gestionar la carga de la red y reducir estos cuellos de botella.

Cuando existen muchos usuarios trabajando con la red, y el sistema de cableado, las tarjetas de red o el servidor no son adecuados, el rendimiento decae, pero también puede suceder con un único usuario si esté se encuentra realizando tareas de cálculo intensivo, utiliza todo el ancho de banda del cable en transmisión de grandes archivos de datos; o realiza una gran parte del procesamiento de datos dentro del servidor, para esto se necesita asignar a este tipo de usuarios su propio tramo de red, o añadir un servidor de uso exclusivo.

Para lograr un buen rendimiento se puede considerar lo siguiente:

- Asegurarse de que el servidor posee memoria RAM suficiente, mínimo 24 Mb.
- Instalar un disco duro de alta capacidad y rendimiento.

- Seleccionar un servidor como un bus de alto rendimiento, como los EISA.
- Utilizar superservidores.
- Instalar tarjetas de red de alto rendimiento en el servidor, con interfaces de 16 ó 32 bits.
- Utilizar tarjetas y cable Ethernet de 10MB/seg o Token Ring de 16Mb/seg, o plantear el utilizar nuevas tecnologías que aumenten el rendimiento como el Fast-Ethernet que maneja velocidades de transmisión de datos de 100 Mb/s con fibra óptica.
- Utilizar sistemas de cableado principal con fibra óptica y ruteadores para conectar los segmentos LAN de alto rendimiento.

4.3. Elección de los elementos de red:

4.3.1. Servidor (NFS, Windows NT, Lan Manager)

La consideración más importante a la hora de adquirir un servidor es el tipo de bus usado en el equipo; el bus es la "autopista" usada para transferir datos entre los componentes del servidor, y entre el servidor, sus tarjetas de red y las estaciones de trabajo. Se clasifican a los servidores entres categorías:

- *Los servidores básicos* son excelentes para redes pequeñas, con 16 Mb en RAM discos duros de 1Gb; estos sistemas utilizan generalmente un bus ISA. Este servidor es un equipo de sobremesa con una sola tarjeta de red para dar servicio a 50 estaciones de trabajo con rendimiento moderado.
- *Los sistemas avanzados* tienen buses de 32 bits EISA, tarjetas de red de alto rendimiento y discos duros más grandes.
- *Los superservidores multiprocesador* son equipos que ofrecen rendimiento varias veces superior a los servidores típicos, un superservidor utiliza un bus especial a velocidades de hasta 250 Mhz, muy superiores a los 12 Mhz del bus ISA. al bus se conectan varios microprocesadores para compartir tareas de procesamiento o ejecutar varias aplicaciones individuales.

Para nuestro diseño se utilizaran los sistemas avanzados para la red LAN, con los siguientes sofwares de red:

NFS Sistema de Archivo de Red (Network File System) Los servidores que contienen este tipo de software de red, tienen sus discos divididos en tres partes básicas:

1- **ROOT:** En esta parte se encuentra el sistema operativo UNIX.

2- **USER:** Aquí se encuentran todas las aplicaciones que serán utilizadas por las estaciones de trabajo, algunas de estas aplicaciones son de uso exclusivo y en otras se puede tener acceso sin restricción.

3- DEV: En esta división se encuentran ligadas todas las impresoras de la red, divididas por piso o por área.

Este tipo de servidor le proporciona al administrador la posibilidad de crear grupos de trabajo por áreas y asignarles a cada una las opciones de lectura, escritura y/o ejecución. Los archivos y las aplicaciones se encuentran encapsulado (1), esto es se encapsulan y esto nos da la seguridad de que si algún archivo tiene virus este virus no se propague a los demás archivos, creando un caos en la red. Se puede tener acceso a la consola del servidor con el servicio de TELNET (2) desde cualquier estación remota.

Aquí cada estación de trabajo debe contar con la licencia de NFS respectiva dentro de su disco duro que será validada por el servidor al tratar de ligarse a él; la configuración del software se vera más adelante. Este software va soportado sobre TCP/IP.

Windows NT: Estos servidores tienen dividido su disco en grupos de trabajo, en los cuales se incluye a los usuarios de cada área, de igual manera como en los servidores NFS; las estaciones de trabajo sólo requieren de un software de red llamado NetBeui para el cual la configuración consta de nombre de computadora, usuario y grupo de trabajo dentro de la red.

Estos servidores son más amigables en cuanto a su configuración, ya que el ambiente de configuración es gráfico y su administración es más sencilla; aquí el principal inconveniente lo tenemos en que la información no se encuentra encapsulada como en los servidores con sistema UNIX, así que podemos tener el problema de tener un archivo con virus y que este se propague a los demás archivos contenidos en el disco duro. El servicio de TELNET para estos servidores requiere de utilizar el protocolo NetBeui con comunicación al NT requerido, accediendo con el súper usuario adecuado, así que cualquier cambio en la configuración del equipo es posible sin desplazarse hasta el equipo (servidor).

Lan Manager Los servidores Lan Manager utilizan sistema operativo UNIX y como software de red TCP/IP de Microsoft; de igual manera NFS tiene dividido también su disco para las diferentes aplicaciones, en este caso la licencia se encuentra en el servidor y no así en las estaciones de trabajo, las cuales solo se configuran con la dirección de la PC, servidor de autentificación y aplicación a la que van a accesar y dirección de correo electrónico si se requiriera. También se puede tener acceso a la consola del servidor a través del software

(1) Encapsulado que significa codificado.

(2) El programa Telnet proporciona capacidad de registro de entrada remoto, esto permite a un usuario de una máquina registrarse en otra, y actuar como si se estuviera frente a la segunda máquina. La conexión puede hacerse desde cualquier parte de una red local, o de otra red en cualquier parte del mundo, siempre y cuando el usuario tenga permiso para registrarse en el sistema remoto. Utiliza para su conexión direcciones IP.

TELNET de cualquier estación de trabajo; se pueden dar los mismos privilegios que en los servidores NFS con sistema operativo UNIX, que son lectura, escritura o ejecución en el disco duro del servidor; esto también puede hacerse en los servidores NT.

Tanto los servidores con software de red NFS, como los que tienen Lan Manager, si alguna de las partes en que esta dividido (ROOT, USER o DEV) se daña, sólo necesitamos volver a instalarla sin que por ello se dejen de dar los demás servicios, lo que no sucede con los servidores que tienen Windows-NT; aquí hay que reinstalar todo y los usuarios dejan de tener acceso a los servicios mientras dure la reinstalación del servidor.

4.3.2. Software TCP/IP (Microsoft TCP/IP, NFS-Pro, NFS-5.0, 3Com TCP)

Microsoft TCP/IP: Este tipo de software de red nos permite tener acceso a la red Internet, identificar al equipo de trabajo, correo electrónico (DNS), y además se encuentra disponible desde la versión de Windows 3.11 en adelante; trabaja bajo Windows y su configuración se verá más adelante. Nos permite acceso a servidores Lan Manager, no así a servidores NFS.

NFS-5.0: Este Software fue creado por SUN-Microsystem para ser instalado bajo el entorno de DOS, a diferencia de NFS-Pro, podemos realizar las ligas a los diferentes servidores que utilizan NFS, desde el mismo sistema operativo, editando algunos comandos y realizando las modificaciones que sean convenientes para accesar a aplicativos que se encuentren en los servidores así como a las impresoras de red, en el caso contrario NFS-Pro las ligas se realizan desde Windows.

Este software se usa en Windows 3.1. y 3.11 solamente.

NFS-Pro: Para este software se requiere tener instalado como mínimo Windows 3.11, puede interactuar con el protocolo NetBeui sin problema alguno, sólo corre bajo entorno Windows.

3Com TCP: Este software no requiere de ninguna licencia, su configuración es menos amigable que en los casos anteriores y puede accesar tanto a servidores Lan Manager, como a servidores NFS; su instalación se realiza desde DOS y solo se puede usar en equipos con Windows 3.1. y 3.11.

Algunas de las configuraciones de estos tipos de software se presentaran más adelante.

4.3.3. Tarjeta de red 3Com:

Existen diferentes fabricantes de tarjetas de red, todas pueden manejar los diferentes protocolos de red cada una tiene un número de identificación que resulta único en el mundo, la diferencia entre ellas se debe en sí a

la velocidad que manejan aquí utilizaremos la tarjeta 3Com, una de las más usadas para una red Ethernet. Este tipo de tarjeta tiene una velocidad de 10 Mbps en la transmisión de datos.

4.3.4.Cableado:

Es importante comprender la instalación del cableado de la red, deberá trazarse un plano de la topología de red incluyendo la situación de los componentes y estaciones de trabajo; evaluar el costo del cable y su instalación.

El rendimiento de la red estará determinado por el número de usuarios en el sistema y el tipo de trabajo que estén realizando; de aquí se desprenderá si es necesario contar con superservidores, que incluyen sistemas de almacenamiento masivo, buses de alta velocidad y varios procesadores, el rendimiento general del sistema depende de varios factores como, cableado (par trenzado, coaxial o fibra óptica), la potencia del servidor (velocidad en mega hertz Mhz), la capacidad del procesador, las estaciones de trabajo y las tarjetas de red.

En nuestro caso de estudio se cuenta con dos servidores HP9000 con sistemas UNIX, los cuales tienen como software de red PCNFS uno y otro con Lan Manager; además se cuenta con un servidor Windows-NT; para tener acceso a cualquiera de los servidores se requiere que cada estación de trabajo tenga un software de red en su disco duro. En el caso del servidor con PCNFS se requiere de una licencia por cada usuario, (NFS5.0 o PCNFS-pro) la cual es grabada directamente en el disco duro de su estación de trabajo y así se puede ingresar a "n" número de usuarios a este servidor (dónde "n" corresponde al número de licencias adquiridas); en el caso de los servidores Lan Manager las licencias se encuentran en él (es decir, la autentificación se lleva a cabo en el servidor), teniendo únicamente que configurar el software de red en la estación de trabajo (TCP/IP), para el servidor Windows-NT sólo requerimos del protocolo NetBeui, y con el tener acceso a los servicios.

La tarjeta que se eligió para unir la PC con el cableado de red y por ende a las demás estaciones de trabajo fue la tarjeta 3com, está es una tarjeta de gran velocidad de transmisión de datos y fácil configuración, con la cual el software NFS trabaja sin ningún contratiempo, así como también el protocolo TCP/IP.

Se tienen dos tipos de cableado:

1- Par trenzado10BaseT, este es utilizado en el Panel de Parcheo, en el concentrador y en las estaciones de trabajo; se eligió debido a que es maleable y de bajo costo, su velocidad de transmisión es de 10Mbps, puede

tener alguna interferencia, su ancho de banda es moderado y tiene una alta fiabilidad en la transmisión de datos.

2- Fibra óptica, este se utiliza para conectar los concentradores con el ruteador ya que su velocidad de transmisión es del orden de miles de Mbps, es inmune a interferencias y normalmente va por tubería para evitar ser dañado (es muy delicado pues la fibra óptica es sumamente delgada).

4.4. Diseño de direccionamiento:

El diseño de direccionamiento se debe hacer de acuerdo a la clase de red que se necesite tener ya sea, A, B, C o D; de acuerdo a la cantidad de equipos a conectar, en la configuración se conoce a la clase como *máscara de subred* (sirve para dividir a una red en subredes), y a cada equipo debe corresponderle un número que lo identifique plenamente dentro de la red (dirección IP), así mismo a cada servidor se le asigna un número y un nombre de identificación único, por ejemplo **9.141.3.6-bus07**, dirección y nombre de servidor respectivamente, esto lo hace el administrador para tener un orden; si hubiera un cambio de lugar de alguno de los equipos (de piso o edificio), tanto de PC's como de servidores se deberá cambiar su dirección de red en cuanto suceda y así evitar contratiempos; esta es una opción y evita perdida de tiempo en el acceso al servidor de autentificación.

Se tienen dos tipos de direcciones:

- ***La dirección de red:*** identifica los segmentos de red, a un mismo servidor pueden estar conectados varios segmentos de red (a través de un ruteador), por ejemplo **9.141.4.10** y **9.142.14.2**, el **141** y **142** representan a dos redes en distintos lugares que pueden estar conectados a un mismo servicio dentro de un servidor.
- ***La dirección de nodo:*** identifica a cada estación de trabajo, dentro de la red que puede ser **9.141.2.15** y **9.141.5.4**, dónde el número **141** nos indica que los equipos se encuentran en el mismo segmento de red y el **2** y **5** nos indican que, el primero corresponde a un equipo que se encuentra en el segundo piso de un edificio y el **5** a otro equipo pero localizado en el quinto.

No existe una regla para realizar el direccionamiento de los equipos; el administrador determina este tipo de direccionamiento.

4.5.Configuración de los equipos:

A continuación se verá la configuración de los equipos, con software de red NFS-Pro (SUN-Microsystem), Lan Manager (TCP/IP de Microsoft) y NFS-5.0. (SUN); para sistemas con Windows 3.1, 3.11 y Windows 95.

TCP/IP Y NFS-Pro son dos paquetes que se instalan desde Windows y requieren de versiones Windows-3.11 en adelante; NFS-5.0 se instala desde sistema operativo DOS, es más comúnmente utilizado en Windows-3.1. Para aprovechar de mejor manera los recursos de estos softwares de red, se recomienda instalar para Windows-3.11 en adelante, ya sea TCP/IP o NFS-Pro, pues estos dos pueden interactuar con otro protocolo de red que es el NETBEUI, pudiendo de esta manera conectar máquinas en red utilizado sólo su nombre, como se vio antes, este protocolo sólo se puede usar dentro de la misma LAN.

4.5.1. Configuración de NFS-Pro:

El software NFS-Pro se puede utilizar con equipos que tengan instalado Windows-3.11 o Windows95. Se instala como sigue; se utilizara la configuración en Windows-95:

1- El software crea un directorio llamado Solarnet.

2- Se entra al icono Red y se agrega el cliente SunSoft-pro, que al mismo tiempo nos agrega el protocolo TCP/IP de SUN Microsystems.

3- En la carpeta identificación, se escribe el nombre de la PC o equipo (Aorozco), el grupo de trabajo al que pertenece (telecom) y la descripción que puede ser el nombre del usuario (Alfonso Orozco).

4- En caso de acceder a un servidor Windows-NT, en la carpeta de control de acceso se da el nombre del servidor (Reforma122) y se dice si es un servidor NT o es un dominio NT.

5- En la carpeta de configuración de Solarnet, en primer lugar se configura el Hostname (nombre de la computadora o número de licencia), su dirección IP (192.100.212.19), el tipo de máscara (255.255.255.128) y el Pasarela (192.100.212.33) al que pertenece el equipo.

6- Si se tiene correo electrónico, se configura el DNS dónde se escribe el dominio al que pertenece (banco_union.com.mx) y la dirección del servidor de correo (192.100.212.61).

7- En el Hosts se escriben las direcciones de los servidores a los que va a accesar el equipo (pueden ser varios).

8- Es necesario en este software tener un nombre de usuario (user6) y una contraseña (puede ser la misma, esto lo determina el administrador), para ligarnos a un servidor de autentificación (el servidor puede ser el 9.141.3.6 cuyo nombre es bun07).

Esta configuración es en esencia la misma aún para Windows-3.11.

4.5.2. Configuración de TCP/IP de Microsoft:

Este software requiere un servidor de autentificación Lan Manager, su configuración es:

1- Dentro de Panel de Control se ejecuta el icono de red.

2- Se selecciona agregar protocolo y se elige TCP/IP de Microsoft.

3- Regresamos al menú principal, seleccionamos TCP/IP y ejecutamos propiedades.

4- Del mismo modo que en el anterior software se escribe una dirección IP.

5- Se escribe el tipo de máscara en la misma carpeta de la dirección IP.

6- Se define el Pasarela que se va a utilizar poniendo la dirección correspondiente.

7- En la carpeta de DNS, se escribe el dominio al que pertenece la máquina y la dirección del servidor de correo (en caso de que la máquina vaya a tener correo o acceso a Internet).

Para este software se tienen que editar dos archivos, el primero es el **hosts.sam** que se encuentra en el directorio **Windows**, y es ahí donde escribimos las direcciones de los servidores a los que queremos accesar (9.141.3.13 CBUNION) y es guardado el cambio con el nombre de **HOSTS**.

El segundo archivo es el **lmhosts.sam**, en la misma ubicación allí se escribe la dirección del servidor de autentificación (200.61.31.3 SIS02 #PRE), este se guarda como **LMHOSTS**.

Como se vio anteriormente en el **HOSTS** se escriben las direcciones de los servidores, esto le sirve al equipo para saber que dirección le corresponde a cada uno de estos y así poder encontrarlos más rápidamente dentro de la red LAN.

4.5.3. Configuración para NFS-5.0:

Este tipo de software es muy utilizado en equipos con sistema operativo Windows 3.1 y 3.11.

La instalación se hace desde DOS, así como también la configuración editando tres archivos que se encuentran en el directorio NFS y son:

1- **HOSTS** (directorio de los servidores), máscara de red, dirección IP, licencia y Pasarela.

9.141.3.2 (dirección IP) PCN123 (licencia)

9.141.3.6(dirección de servidores) bun07 (nombre del servidor)

9.141.3.3 bun14

9.141.3.200(dirección del ruteador) Reforma364 (nombre del ruteador)

2- **NETWORK.BAT** (servidor de autentificación).

NET START RDR LIC123

NET SUBNET 255.255.0.0 (máscara de red)

NET PCNFSD bun07 (servidor de autentificación

NET ROUTE Reforma364

NET LOGIN user6 (login) user6(contrasefia de red)

3- **DRIVES.BAT** (liga a los servidores y a la impresora).

NET USE F: bun07:/users/office (servicio a utilizar)

NET USE lpt1: bun07:prtp_19_2 (servidor y nombre de la impresora de red)

También se deben hacer modificaciones a los archivos **autoexec.bat** y **config.sys**, estos cambios hacen referencia a los archivos de red que se están implementando y son:

Autoexec.bat

SET TZ=CST6

PATH C:\NFS;C:\LANMAN; %PATH%

SET NFSDRIVE=C

C:\LANMAN\NETBIN

SET NFSPATH=C:\NFS\TELNET

LH C:\NFS\PRT

LH C:\NFS\NET –q INIT

LH C:\NFS\rtm /HEAP 64

Config.sys

BREAK ON

DEVICEHIGH=C:\LANMAN\PROTMAN.SYS

DEVICEHIGH=C:\LANMAN\ELNK3.DOS

DEVICEHIGH=C:\NFS\PCNFS.SYS

DEVICEHIGH=C:\NFS\SOCKDRV.SYS

DEVICEHIGH=C:\LANMAN\NFS-NDIS.SYS

LASTDRIVE=Z

La diferencia entre NFS-5.0 Y NFS-Pro radica en que, el NFS-Pro puede interactuar con el protocolo NetBeui de manera natural y al NFS-5.0 se le deben hacer modificaciones además que Pro sólo crea una línea que es:

CALL C:\SOLARNET\ETC\NFSWAUTO

Dónde en el ETC se encuentra el HOSTS y todo lo concerniente a su configuración y el NFSWAUTO realiza la verificación, mediante diversos procedimientos del número de licencia y dirección de red; si encontrara algo mal o que se repitieran cualquiera de los dos, nos desplegaría un mensaje de error antes de entrar a Windows.

4.6. Problemas y soluciones más comunes:

Existe un comando llamado **ping** (Packet Internet Groper), es el método más sencillo para verificar la conexión de una máquina con la red; utiliza el protocolo **Internet de Control de Mensajes** (ICMP) para enviar una solicitud de respuesta, así se puede verificar si tenemos conexión con el enrutador y con los servidores por ejemplo se escribe desde DOS: ping 9.141.3.200 si se obtiene respuesta se dice que se está viendo la red.

Problema con la tarjeta de red: los problemas más comunes son una tarjeta defectuosa o un conector malo, la verificación de la tarjeta puede hacerse aplicándole un test, que es proporcionado por el fabricante a través de un disquete de computadora, para ello debemos montarla dentro de la PC dónde se va a utilizar. En el caso del conector malo se utiliza un analizador de protocolos que va conectado a uno de los extremos del cable, manda señales y verifica la recepción de las mismas.

Si las conexiones de red y las tarjetas de red aparentemente funcionan correctamente, el problema corresponde a una capa superior.

Otro problema común con las tarjetas de red, se debe a la mala configuración de la tarjeta, está debe configurarse en el momento de instalar el sistema operativo para que este la reconozca y la active al momento de iniciarse. En algunas ocasiones debemos jugar un poco con la configuración de la tarjeta de red.

Problemas en la capa IP: Debido a que en esta capa se da el enrutamiento, cualquier error puede causar pérdida de información. Uno de los errores más comunes es, la duplicidad de direcciones IP, la máscara de

subred también debe ser correcta, es decir debe corresponder a la clase de red que se tenga en ese momento; esto se corrige verificando y haciendo los cambios necesarios en la configuración del software de red que se requiera.

Se pueden tener problemas debido al tipo de software que se este utilizando si no son idénticos o compatibles el problemas se vuelve difícil de resolver, esto ocurre particularmente en plataformas mixtas, como FTP Protocolo de Transferencia de Archivos (File Transfer Protocol) basado en PC o un paquete de software TCP/IP tratando de tener acceso a un anfitrión UNIX con software NFS.

También se pueden tener problemas de conexión a la red si el usuario no se autentifica, esto es válido para NFS (en sus dos versiones), TCP/IP de Microsoft , NT y Netbeui.

Se pueden tener problemas para acceso en servidores Lan Manager o NT, cuando se ha cumplido con la cantidad de usuarios permitidos para acceder a ellos.

En cuanto a las impresiones se puede tener problemas con estas, si los servidores dedicados a administrar dichas impresiones se saturan por la cantidad de trabajos a imprimir, esto es que los archivos que se mandan a impresión son demasiado grandes, por ejemplo de 8 Mb.

A ABREVIATURAS.

ARP .....– Protocolo de Resolución de Dirección

ARPA .....– Agencia de Proyectos de Investigación Avanzada

CSMA/CD .....– Acceso Múltiple de Percepción de Portadora con Detección de Colisión

DNS .....– Sistema de Nombre de Dominio

DO S.....– Sistema Operativo de Disco

FTP .....– Protocolo de Transferencia de Archivos

ICMP .....– Protocolo Internet de Control de Mensajes

IP .....– Protocolo Internet

ISO .....– Organización Internacional para la Estandarización

LAN .....– Red de Area Local

LLC .....– Control de Vínculo Lógico

LSAP .....– Dirección de la Capa de Vínculo de Datos

MAC .....– Control de Acceso al Medio

MAN .....– Red de Area Metropolitana

MAU .....– Unidad de Acceso Multiestación

NFS .....– Sistema de Archivos de Red

NIC .....– Tarjeta de Interfaz de Red

OSI .....– Interconexión de Sistemas Abiertos

OSPF .....– Abrir Primero Trayectoria más Corta

OS/2 .....– Sistema Operativo /2

PING .....– Buscador de Paquetes Internet

RDC .....– Red De Computadoras

RIP .....– Protocolo de Información de Enrutamiento

SNMP .....– Protocolo Simple de Administración de Red

SPX/IPX .....– Secuencia de Intercambio de Paquetes/Intercambio de Paquetes en red Interna

TCP .....– Protocolo de Control de Transmisión

TELNET .....- Red Terminal

UDP .....- Protocolo de Datagrama de Usuario

WAN .....- Red de Area Amplia

XNS .....- Sistemas de Red Xerox

B GLOSARIO.

Arc Net. Es un tipo de red, que utiliza una topología de red en estrella o bus con acceso por pase de testigo.

DEV. Es la parte del servidor UNIX donde se encuentran los nombres y direcciones de los equipos periféricos como son Modems, Impresoras, Puertos, etc.

EISA. Sistema Adaptador de Interconexiones Extendido.

Ethernet. Es una topología de red en bus lineal con método de acceso CSMA/CD.

Gateway (compuerta). En términos de Internet una compuerta es un dispositivo que enruta datagramas. En forma más reciente este término se empleo para referirse a cualquier dispositivo de red que traduce protocolos de un tipo de red a otros de una red diferente.

Hardware. Parte física de los equipos PC's, impresoras, etc.

Hosts. Archivo donde se relacionan nombres y direcciones de servidores.

Hub. Conmutador de red que acondiciona y amplifica la intensidad de la señal.

Internetwork (interred). Red interna.

ISA. Sistema Adaptador de Interconexiones.

Login. Se encuentran en esta parte de UNIX los atributos y direcciones de los usuarios.

Macintosh. Sistema operativo de Apple.

NetBeui. Protocolo de comunicación no enrutable para comunicación entre PC's.

Nodo. Término genérico que se usa para referirse a los dispositivos finales de red.

Protocolo. Reglas que gobiernan el comportamiento o el método de operación de algo.

ROOT. Raíz del sistema operativo UNIX.

Router (ruteador). Dispositivo que conecta LANS en una interred y enruta tráfico entre estas.

Software. Es la parte de la programación de los equipos.

Token Ring. Es una red en anillo por pase de testigo, se puede configurar en estrella.

Topología. Es la organización del cableado en una red (bus, anillo, estrella o combinación de ellas).

UNIX. Sistema operativo enfocado a la creación de redes.

USER. Se encuentra en el, el directorio de las aplicaciones que serán usadas por los usuarios, (office o aplicaciones especiales).

10 Base-T. Término de Ethernet que se refiere a una velocidad máxima de transferencia de información de 10 Mbps. La cual usa señalización de banda base y cableado de par trenzado.

CONCLUSION

Con la realización de esta tesis me encontré, con información referente al protocolo TCP/IP muy técnica o en idioma ingles; por lo que se hace más difícil la comprensión de esta herramienta que es la más usada para la comunicación a nivel mundial por Internet.

En la parte educativa, los estudiantes de las carreras afines no conocen del todo este protocolo, su definición o incluso su configuración básica a nivel de usuario, así que cuando se enfrentan al trabajo, les es difícil entender su funcionamiento. Es por esto que sé pensó en la realización de un trabajo que trate el tema de TCP/IP desde un punto de vista menos técnico (en la medida de lo posible), para que no sólo los estudiantes, sino que también otras personas aunque no estén relacionadas con el tema lo puedan comprender en su mayor parte.

Aquí se descubren las bondades del protocolo, su alta eficiencia y la optimización de los recursos, con lo cual Se abaten costos ya que podemos compartir diferentes periféricos, los cuales son utilizados por varias personas a la vez.

BIBLIOGRAFIA:

Título: Telecomunications (Protocols and Desing)

Autores: John D. Spragins

Joseph L. Hammond

Krzystof Pawlikowski

Editorial: Addison-Wesley Publishing Company

Título: Data Network Desing

Autor: Darren L. Spohn

Editorial: McGraw-Hill

Título: Interworking with TCP/IP Volumen I

Autor: Douglas E. Coner

Editorial: Prentice Hall

Título: Telecommunication Networks

Autor: Mischa Schwartz

Editorial: Addison-Wesley Publishing Company

Título: Communications for cooperating systems

Autor: R. J. Cypser

Editorial: Addison- Wesley Publishing Company

Título: Internet Manual de Referencia

Autores: Harley Hahn

Rick Stout

Editorial: Osborne McGraw-Hill

Título: Computer Networks Protocols, Standars and Interfaces

Autor: Uyless Black

Editorial: Prentice Hall Segunda Edición

Título: TCP/IP and NFS Interworking in a UNIX Enviroment

Autor: Michael Santifalled

Editorial: Addison-Wesley Publishing Company

Título: Understanding TCP/IP

Autor: 3Com Education Services

Editorial: Manual Publicado para 3Com

Título: Data Networks

Autor: Uyless Black

Editorial: Prentice Hall

Título: Aprendiendo TCP/IP

Autor: Timothy Parker

Editorial: Prentice Hall