

**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**  
**FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**



**UNIVERSIDAD NACIONAL**  
**AUTÓNOMA DE**  
**MÉXICO**

**“SOFTWARE DE ADMINISTRACIÓN DE REDES LAN Y TEMAS DE APOYO  
PARA LA MATERIA DE REDES DE COMPUTADORAS”**

**TESIS**  
**QUE PARA OBTENER EL TÍTULO DE**  
**ING. EN COMPUTACIÓN**  
**PRESENTA:**

**RICARDO RAMIREZ MORA**

**MEXICO 2011**



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## **DEDICATORIAS Y AGRADECIMIENTOS**

### **A mis padres**

Por su cariño y apoyo sin condiciones, me han enseñado a encarar las adversidades sin desfallecer en el intento, me han dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño y todo ello sin pedir nunca nada a cambio.

Gracias por confiar en mí y darme la oportunidad de culminar esta etapa de mi vida.

### **A mi hermano**

Por la compañía y el apoyo que me brinda. Sé que cuento con el siempre.

### **A Claudia**

Por su paciencia, por su comprensión, por su cariño, que me permite sentir que puedo lograr lo que me proponga, pero sobre todo gracias por enseñarme a creer en mí y motivarme a hacer las cosas de la mejor manera.

### **A mis profesores**

Por compartirme sus conocimientos y por el tiempo que me han dedicado para leer este trabajo.

## ÍNDICE

<b>INTRODUCCIÓN</b> .....	6
<b>CAPITULO I. ANTECEDENTES DE REDES LAN</b> .....	7
1.1 Redes de área local (LAN) .....	8
1.1.1 Evolución .....	8
1.2 Componentes básicos de las redes de computadoras .....	9
1.2.1 El ordenador .....	9
1.2.2 Tarjetas de red .....	9
1.3 Tipos de servidores .....	10
1.4 ¿Por qué usar una red? .....	12
1.4.1 Ventajas .....	12
1.5 La expansión de las redes .....	12
1.6 Tipos de redes .....	13
1.6.1 Ethernet .....	14
1.6.2 Token Ring .....	14
1.6.3 Arcnet .....	14
1.7 Clasificación de redes .....	17
1.8 El concepto de Networking .....	18
<b>CAPITULO II. PROTOCOLOS</b> .....	20
2.1 El modelo OSI .....	21
2.1.1 Historia .....	21
2.1.2 Normalización dentro del modelo OSI .....	23
2.1.3 Primitivas de servicio y parámetros .....	23
2.1.4 Modelo de referencia OSI .....	23
2.2 Los elementos que definen un protocolo .....	27
2.3 Como trabajan los protocolos .....	27
2.3.1 El ordenador emisor .....	28
2.3.2 El ordenador receptor .....	28
2.4 Protocolos en una arquitectura en niveles .....	29
2.4.1 Stacks de protocolos .....	29
2.5 Propiedades típicas de los protocolos .....	29

2.6	Funciones de los protocolos .....	30
2.7	Protocolos más importantes .....	33
2.7.1	El Protocolo TCP/IP .....	34
2.7.2	IP .....	43
2.7.3	El protocolo NETBEUI .....	46
2.7.4	El protocolo IPX/SPX .....	49
2.8	Un modelo de tres capas .....	52
2.9	Protocolos ruteables VS no ruteables .....	53

### **CAPITULO III. TOPOLOGÍAS DE RED, MÉTODOS DE ACCESO Y MEDIOS DE TRANSMISIÓN .....**

3.1	Topologías de red .....	54
3.1.1	Topología jerárquica .....	55
3.1.2	Topología horizontal .....	56
3.1.3	Topología en estrella .....	58
3.1.4	Topología en anillo .....	59
3.1.5	Topología malla .....	60
3.1.6	Variaciones en las principales topologías .....	61
3.2	Métodos de acceso .....	64
3.2.1	Clasificación métodos de acceso .....	65
3.3	Medios de transmisión .....	68
3.3.1	Principales tipos de cables .....	68
3.3.2	Cable coaxial .....	69
3.3.3	Cable de par trenzado .....	71
3.3.4	UTP. Par trenzado no blindado (no aislado) .....	72
3.3.5	STP. Par trenzado aislado .....	73
3.3.6	FTP. Par trenzado con blindaje global .....	74
3.3.7	Cable de fibra óptica .....	75

<b>CAPITULO IV. SOFTWARE PARA LA ADMINISTRACIÓN DE REDES LAN...</b>	<b>79</b>
4.1	Objetivos de la administración de redes LAN ..... 79
4.1.1	Elementos involucrados en la administración de red ..... 81
4.1.2	Operaciones de la administración de red ..... 81
4.1.3	Funciones de administración definidas por OSI ..... 84
4.1.4	Administración definida por snmp ..... 86
4.1.5	Base de datos de administración: mib ..... 89
4.1.6	Seguridad en la administración de redes ..... 91
4.1.7	Software para administrar redes LAN ..... 92
<b>CONCLUSIONES</b>	..... 110
<b>BIBLIOGRAFÍA</b>	..... 112
<b>GLOSARIO</b>	..... 114

## INTRODUCCIÓN

La industria de las computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una computadora para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información.

Las redes en general, sirven para compartir recursos y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 100 m de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Este trabajo está realizado con la finalidad de ser utilizado como material de apoyo para la materia de redes de computadora y está dirigido principalmente para todos los estudiantes de la carrera de ingeniería en computación que estén interesados en conocer con más detalle los temas relacionados con las redes LAN.

En éste trabajo se hablará de los fundamentos de las redes de computadoras y principalmente de las redes LAN, para que las personas que lean esta tesis sepan un poco más de este tema, además se hablará de qué es una red y para qué sirve, cómo opera y algunos tipos de protocolos.

También se responderán algunas de las preguntas más frecuentes sobre la red, los tipos de red, por qué usar una red, y más preguntas por el estilo.

Están incluidas algunas imágenes que servirán para un mejor entendimiento y para una mejor comprensión. Y por último se mostraran algunos ejemplos de software para la administración de redes LAN.

## CAPÍTULO I

### ANTECEDENTES Y CONCEPTOS BÁSICOS DE REDES LAN.

El inicio del uso de redes locales, a finales de la década de 1970, fue un hecho significativo en el desarrollo del campo de la computación. Estas redes fueron desarrolladas por ingenieros que advirtieron que el empleo de técnicas de computación, más que de técnicas de telecomunicaciones, permitiría obtener grandes anchos de banda, bajas tasas de error y bajo costo. Las nuevas redes locales de banda ancha llegaron justamente cuando se les necesitaba, para permitir que las computadoras de bajo costo, que se estaban instalando en grandes cantidades, pudieran compartir periféricos; al mismo tiempo, hicieron posible un nuevo enfoque del diseño de sistemas compartidos de computación.

Debido a la creciente cantidad de computadoras, se llegó a la necesidad de la comunicación entre ellas para el intercambio de datos, programas, mensajes y otras formas de información. Las redes de computadoras llegaron para llenar esta necesidad, proporcionando caminos de comunicación entre las computadoras conectadas a ellas.

Con el aumento de sistemas de computación y del número de usuarios potenciales, se llegó a la necesidad de un nuevo tipo de redes de comunicaciones. Al principio, las redes de área extendida (WAN, Wide Area Network), también conocidas como grandes redes de transporte, fueron un medio de conexión de terminales remotas a sistemas de computación. En estos sistemas de conexión, los dispositivos pueden funcionar como unidades independientes y se conectan por una red que cubre una gran área. Los medios de comunicación usados para la red pueden ser líneas telefónicas o cables tendidos específicamente para la red.

Las velocidades requeridas para tales sistemas pueden ser bastante lentas. Como el tamaño de los mensajes suele ser grande, el tiempo para recibir el reconocimiento puede ser largo. Las velocidades de operación típicas de este tipo de redes están en el intervalo de 10 a 50 Kbps, con tiempos de respuesta del orden de algunos segundos.



Se trata de redes de conmutación de paquetes que usan nodos de conmutación y el método de operación de almacenamiento y reenvío.

La cantidad de sistemas computarizados ha crecido debido a los avances en microelectrónica, lo que ha dado lugar a la necesidad de un nuevo tipo de red de computadoras, llamada red de área local (LAN, Local Area Network). Las redes de área local se originaron como un medio para compartir dispositivos periféricos en una organización dada. Como su nombre lo indica, una red local cubre un área geográfica limitada y su diseño se basa en un conjunto de principios diferentes a los de las redes de área extendida.

## **1.1 REDES DE ÁREA LOCAL (LAN)**

Las redes empezaron siendo pequeñas, con quizás 10 ordenadores conectados junto a una impresora. La tecnología limitaba el tamaño de la red, incluyendo el número de ordenadores conectados, así como la distancia física que podría cubrir la red. Por ejemplo, en los primeros años 80 el más popular método de cableado permitía como 30 usuarios en una longitud de cable de alrededor de 200 metros (600 pies). Por lo que una red podía estar en un único piso de oficina o dentro de una pequeña compañía. Para muy pequeñas empresas, hoy ésta configuración es todavía adecuada. Este tipo de red, dentro de un área limitada, es conocida como una red de área local (LAN).

### **1.1.1 Evolución**

Las primeras redes fueron de tiempo compartido, las mismas que utilizaban mainframes y terminales conectadas.

Dichos entornos se implementaban con la SNA (Arquitectura de Sistemas de Redes) de IBM (international business machines) y la arquitectura de red Digital.

Las LAN permitieron que usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos, y tener acceso a recursos compartidos de toda la Red, tales como Servidores de Archivos o de aplicaciones.

Con la aparición de Netware surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. Netware dominaba el campo de las LAN de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups.

Microsoft y 3Com trabajaron juntos para crear un sistema operativo de red simple el cual estaba formado por la base de 3Com's 3+Share, el Gestor de redes LAN de Microsoft y el Servidor del IBM. Ninguno de estos proyectos fue muy satisfactorio.

## **1.2 COMPONENTES BÁSICOS DE LAS REDES DE COMPUTADORAS**

### **1.2.1 El ordenador**

La mayoría de los componentes de una red media son los ordenadores individuales, también denominados host; generalmente son sitios de trabajo (incluyendo ordenadores personales) o servidores.

### **1.2.2 Tarjetas de red**

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarojos ó radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red o NIC (Network Card Interface) con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras

computadoras, empleando un protocolo para su comunicación y convirtiendo esos datos a un formato que pueda ser transmitido por el medio (bits 0's/1's). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC (Media Access Control), que consta de 48 bits (6 bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuados.

El trabajo del adaptador de red es el de permitir la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras (discos duros, impresoras, etc.). Estos adaptadores son unas tarjetas PCI que se conectan en las ranuras de expansión del ordenador. En el caso de ordenadores portátiles, estas tarjetas vienen en formato PCMCIA. En algunos ordenadores modernos, tanto de sobremesa como portátiles, estas tarjetas ya vienen integradas en la placa base.

Adaptador de red es el nombre genérico que reciben los dispositivos encargados de realizar dicha conversión. También las velocidades disponibles varían según el tipo de adaptador; éstas pueden ser, en Ethernet, de 10, 100 ó 1000 Mbps y en los inalámbricos de 11 ó 55 Mbps.

### **1.3 TIPOS DE SERVIDORES**

En la siguiente lista hay algunos tipos comunes de servidores y sus propósitos.

- Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.
- Servidor de impresiones: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.

- Servidor de correo: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con e-mail para los clientes de la red.
- Servidor de fax: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
- Servidor de la telefonía: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet.
- Servidor proxy: Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web. Además realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., depositar documentos u otros datos que se soliciten muy frecuentemente).
- Servidor del acceso remoto (RAS): controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.
- Servidor Web: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.
- Servidor DNS: Este tipo de servidores resuelven nombres de dominio sin necesidad de conocer su dirección IP.
- Otros dispositivos: hay muchos otros tipos de dispositivos que se puedan utilizar para construir una red, muchos de los cuales requieren una comprensión de conceptos más avanzados del establecimiento de una red de la computadora antes de que puedan ser entendidos fácilmente (los cubos, las rebajadoras, los puentes, los interruptores, los cortafuegos del hardware, etc.). En las redes caseras y móviles, que conecta la electrónica de consumidor los dispositivos tales como consolas de vídeo juegos está llegando a ser cada vez más comunes.

## **1.4 ¿PORQUÉ USAR UNA RED?**

Las organizaciones implementan redes principalmente para compartir recursos y habilitar comunicación online. Los recursos incluyen datos, aplicaciones y periféricos. Un periférico es un dispositivo como un disco externo, impresora, ratón, modem o joystick. Comunicación Online incluye enviar mensajes de un lugar a otro, o e-mail.

### **1.4.1 Ventajas**

En una empresa suelen existir muchos ordenadores, los cuales necesitan de su propia impresora para imprimir informes (redundancia de hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican (redundancia de datos), los ordenadores que trabajen con los mismos datos deberán de tener los mismos programas para manejar dichos datos (redundancia de software), etc.

## **1.5 LA EXPANSIÓN DE LAS REDES**

Las primeras LAN no podían soportar adecuadamente las necesidades de grandes negocios con oficinas en varios lugares. Como las ventajas del networking llegaron a ser conocidas y más aplicaciones fueron desarrolladas para entorno de red, los empresarios vieron la necesidad de expandir sus redes para mantenerse competitivos.

Así como el ámbito geográfico de la red crece conectando usuarios en diferentes ciudades o diferentes estados, la LAN crece en una Red de Área Amplia (WAN). El número de usuarios en la red de una compañía puede ahora crecer de 10 a miles.

Hoy, la mayoría de los negocios más importantes almacenan y comparten vastas cantidades de datos cruciales en un entorno de red, que es por lo que las redes son actualmente tan esenciales para los empresarios como las mecanógrafas y los archivos lo fueron.

La solución a estos problemas se llama red de área local, esta permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat.

Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Además una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varios ordenadores conectados en red.

## **1.6 TIPOS DE REDES**

La oferta de redes de área local es muy amplia, existiendo soluciones casi para cualquier circunstancia. Podemos seleccionar el tipo de cable, la topología e incluso el tipo de transmisión que más se adapte a nuestras necesidades. Sin embargo de toda esta oferta las soluciones más extendidas son tres: Ethernet, Token Ring y Arcnet.

### **1.6.1 Ethernet**

La red Ethernet usa una topología de bus donde todos los computadores están conectados por un cable de alta velocidad (de hasta 100 Mbps). Si más de una computadora envía información al mismo tiempo las señales colisionan y se pierde información.

Para evitar esto, Ethernet utiliza una técnica de contención MAC, llamada: Carrier sense multiple access/collision detection (CSMA/CD).

Con esta técnica, cada computadora de la red, puede enviar información a la red en cualquier momento, pero antes de enviar los datos, deben asegurarse de que la red no esté en uso.

Los datos se envían sólo cuando se asegura de que ningún otro dato ha sido enviado.

### **1.6.2 Token Ring**

Token Ring es una arquitectura de red desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo, usando un frame de 3 bytes llamado token que viaja alrededor del anillo. En estos tiempos está en desuso por la popularización de Ethernet; actualmente no es empleada en diseños de redes.

### **1.6.3 Arcnet**

La Red de computación de recursos conectadas (ARCNET, Attached Resource Computing Network) es un sistema de red banda base, con paso de testigo (token) que ofrece topologías flexibles en estrella y bus a un precio bajo. Las velocidades de transmisión son de 2.5 Mbits/seg. ARCNET usa un protocolo de paso de testigo en una topología de red en bus con testigo.

En 1981, Standard Microsystems Corporation (SMC) desarrollo el primer controlador LAN en un solo chip basado en el protocolo de paso de testigo de ARCNET.

Es adecuada para entornos de oficina que usan aplicaciones basadas en texto y donde los usuarios no acceden frecuentemente al servidor de archivos. Las versiones más nuevas de ARCNET soportan cable de fibra óptica y de par-trenzado.

A continuación se explican otros tipos de redes:

- Red pública: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.
- Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.
- Red de área Personal (PAN): (Personal Area Network) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.



- Red de área local virtual (VLAN): Una Virtual LAN ó comúnmente conocida como VLAN, es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física.

Con esto, se pueden lógicamente agrupar computadoras para que la localización de la red ya no sea tan asociada y restringida a la localización física de cada computadora, como sucede con una LAN, otorgando además seguridad, flexibilidad y ahorro de recursos. Para lograrlo, se ha establecido la especificación IEEE 802.1Q como un estándar diseñado para dar dirección al problema de cómo separar redes físicamente muy largas en partes pequeñas, así como proveer un alto nivel de seguridad entre segmentos de redes internas teniendo la libertad de administrarlas sin importar su ubicación física.

- Red del área del campus (CAN): Se deriva a una red que conecta dos o más LAN los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.
- Red de área metropolitana (MAN): una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores (routers) múltiples, los interruptores (switch) y los cubos están conectados para crear a una MAN.
- Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono.

- Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de enlace de datos, y la capa de red.

## 1.7 CLASIFICACIÓN DE REDES

- Por alcance:
  - Red de área personal (PAN)
  - Red de área local (LAN)
  - Red de área de campus (CAN)
  - Red de área metropolitana (MAN)
  - Red de área amplia (WAN)
  - Red de área de almacenamiento (SAN)
- Por método de la conexión:
  - Medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.
  - Medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas.
- Por relación funcional:
  - Cliente-servidor
  - Igual-a-Igual (p2p)
- Por Topología de red:
  - Red en bus
  - Red en estrella
  - Red en anillo (o doble anillo)
  - Red en malla (o totalmente conexa)
  - Red en árbol
  - Red mixta (cualquier combinación de las anteriores)

- Por la direccionalidad de los datos (tipos de transmisión)
  - Simplex (unidireccionales): un Equipo Terminal de Datos transmite y otro recibe.
  - Half-Duplex (bidireccionales): sólo un equipo transmite a la vez. También se llama Semi-Duplex (p. ej. una comunicación por equipos de radio).
  - Full-Duplex (bidireccionales): ambos pueden transmitir y recibir a la vez una misma información. (p. ej. videoconferencia).

## 1.8 EL CONCEPTO DE NETWORKING

Networking puede definirse como un conjunto de hardware y software de gestión necesario para la conexión de múltiples ordenadores con el fin de que puedan intercambiar información entre ellos y compartir recursos.

En su nivel más elemental, una red consiste en dos ordenadores conectados mediante un cable para que puedan compartir datos. Todo el networking, no importa cuán sofisticado, procede de ese simple sistema.

Mientras la idea de dos ordenadores conectados por cable puede no parecer extraordinaria, en retrospectiva, fue un gran logro en comunicaciones.

Networking surge de la necesidad de compartir datos en una forma oportuna. Los ordenadores personales son buenas herramientas de trabajo para producir datos, hojas de cálculo, gráficos y otros tipos de información, pero no te permiten compartir rápidamente los datos que has producido. Sin una red, los documentos tienen que ser impresos para que otros los editen o los usen. En el mejor de los casos, entregas ficheros en diskettes a otros para que los copien a sus ordenadores. Si otros hacen cambios en el documento no hay manera de mezclarlos. Esto fue, y todavía es, llamado trabajo en un entorno aislado. (Stand alone).

Networking → trabajo en red → compartición de datos, impresoras, módems, faxes, gráficos...

LAN → varios pc's que corresponden a una única ubicación física. Solo se utiliza un medio (cable)

WAN → redes distintas.

Porqué usar una red: en términos económicos → compartir hardware.

En términos de datos → compartir aplicaciones (un schedule o agenda)

Si un trabajador aislado conectase su ordenador a otros ordenadores, podría compartir los datos en los otros ordenadores e impresoras.

Un grupo de ordenadores y otros aparatos conectados juntos es llamado una red, 'network', y el concepto de ordenadores conectados compartiendo recursos es llamado 'networking'.

Como se ha visto en este primer capítulo se trataron algunos conceptos básicos acerca de las redes de computadoras, tipos y clasificaciones además de dar una breve descripción acerca de las redes LAN. Ahora se definirá el concepto de protocolos en el siguiente capítulo.

## **CAPÍTULO II**

### **PROTOCOLOS**

El Protocolo de red o también Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

El uso de las reglas de comunicación se aplica de la misma manera en el entorno de los ordenadores. Cuando varios ordenadores están en red, las reglas y procedimientos técnicos que gobiernan su comunicación e interacción se llaman protocolos.

Hay 3 puntos a tener en cuenta cuando se piensa en protocolos en un entorno de red:

1. Hay varios protocolos. Mientras cada protocolo permite comunicaciones básicas, tienen propósitos diferentes y realizan tareas diferentes. Cada protocolo tiene sus propias ventajas y restricciones.
2. Algunos protocolos trabajan en varios niveles OSI. El nivel en el que trabaja un protocolo describe su función.

Por ejemplo, un cierto protocolo trabaja en el nivel Físico, significando que el protocolo en ese nivel asegura que el paquete de datos pasa a través de la tarjeta de red y sale al cable.

3. Varios protocolos pueden trabajar juntos en los que es conocido como un stack de protocolos, o suite.

Antes de adentrarnos más en el tema de protocolos es importante explicar primero el sistema OSI, es por eso que primero lo definiremos para entender algunas cosas con respecto a los protocolos.

## 2.1 EL MODELO OSI

El modelo de interconexión de sistemas abiertos, también llamado OSI (en inglés open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984.

Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

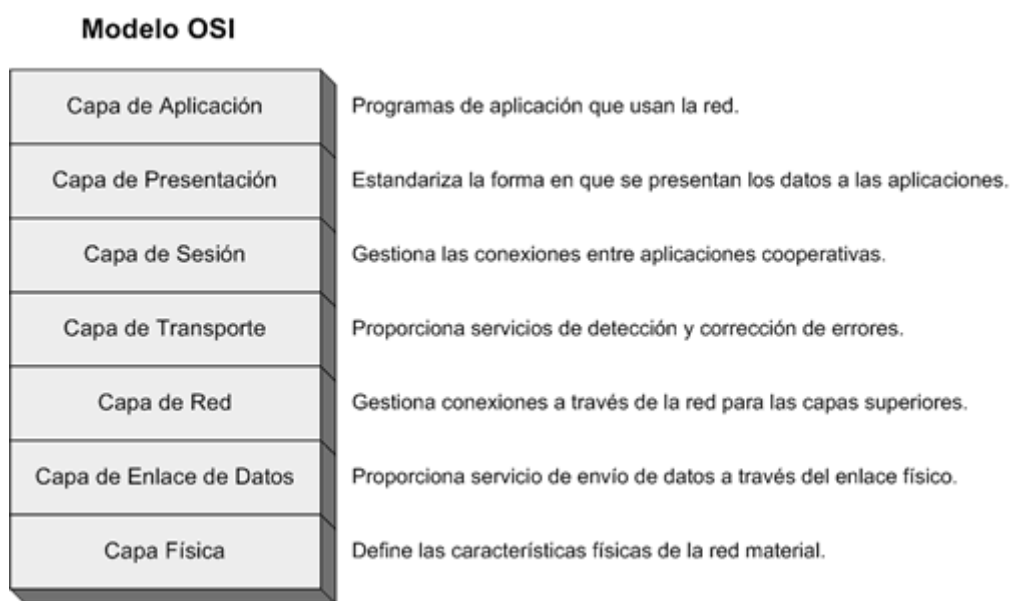


Fig. 1

Modelo OSI

### 2.1.1 Historia del modelo OSI

A principios de 1980 el desarrollo de redes sucedió con desorden en muchos sentidos. Se produjo un enorme crecimiento en la cantidad y tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión.

De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información.

El mismo problema surgía con las empresas que desarrollaban tecnologías de conexiones privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología. Las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de conexión como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes.

Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El sistema de comunicaciones del modelo OSI estructura el proceso en varias capas que interaccionan entre sí. Una capa proporciona servicios a la capa superior siguiente y toma los servicios que le presta la siguiente capa inferior.

De esta manera, el problema se divide en subproblemas más pequeños y por tanto más manejables.

Para comunicarse dos sistemas, ambos tienen el mismo modelo de capas. La capa más alta del sistema emisor se comunica con la capa más alta del sistema receptor, pero esta comunicación se realiza vía capas inferiores de cada sistema. La única comunicación directa entre capas de ambos sistemas es en la capa inferior (capa física).

Los datos parten del emisor y cada capa le adjunta datos de control hasta que llegan a la capa física. En esta capa son pasados a la red y recibidos por la capa física del receptor. Luego irán siendo captados los datos de control de cada capa y pasados a una capa superior. Al final, los datos llegan limpios a la capa superior.

Cada capa tiene la facultad de poder trocear los datos que le llegan en trozos más pequeños para su propio manejo. Luego serán reensamblados en la capa paritaria de la estación de destino.

### **2.1.2 Normalización dentro del modelo OSI**

El proceso de descomposición del problema de comunicaciones en capas hace posible la normalización de cada capa por independiente y la posible modificación de una capa sin afectar a las demás.

Es preciso el empleo de normalizaciones para que dos sistemas puedan conocerse y poder comunicarse con plena exactitud, sin ambigüedades.

Para que dos capas de dos sistemas se puedan comunicar es necesario que estén definidas las mismas funciones en ambos, aunque el cómo se implementen en la capa inferior de cada sistema sea diferente.

### **2.1.3 Primitivas de servicio y parámetros**

Las capas inferiores suministran a las superiores una serie de funciones o primitivas y una serie de parámetros. La implementación concreta de estas funciones está oculta para la capa superior., ésta sólo puede utilizar las funciones y los parámetros para comunicarse con la capa inferior (paso de datos y control).

### **2.1.4 Modelo de referencia OSI**

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.



El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas:

### **Capa física (Capa 1)**

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

## **Capa de enlace de datos (Capa 2)**

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Se hace un direccionamiento de los datos en la red ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores, de la topología de la red de cualquier tipo.

## **Capa de red (Capa 3)**

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores, aunque es más frecuente encontrar el nombre inglés routers y, en ocasiones enrutadores.

Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

## **Capa de transporte (Capa 4)**

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento. Sus protocolos son TCP y UDP el primero orientado a conexión y el otro sin conexión.

### **Capa de sesión (Capa 5)**

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre los dos computadores que están transmitiendo datos de cualquier índole.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

### **Capa de presentación (Capa 6)**

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

### **Capa de aplicación (Capa 7)**

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

Una vez que hemos definido el concepto del modelo OSI ahora procederemos a continuar con el tema de protocolos.

## **2.2 LOS ELEMENTOS QUE DEFINEN UN PROTOCOLO SON:**

- Sintaxis: formato, codificación y niveles de señal de datos.
- Semántica: información de control y gestión de errores.
- Temporización: coordinación entre la velocidad y orden secuencial de las señales.

## **2.3 COMO TRABAJAN LOS PROTOCOLOS**

La totalidad de la operación técnica de transmitir datos por la red tiene que ser rota en pasos discretos y sistemáticos. En cada paso, ciertas acciones tienen lugar porque no lo tienen en cualquier otro paso. Cada paso tiene sus propias reglas y procedimientos, o protocolo.

Los pasos tienen que ser llevados a cabo en un orden consistente que es el mismo en cada ordenador de la red.

### **2.3.1 El ordenador emisor**

En el ordenador emisor, el protocolo:

- Rompe el dato en secciones más pequeñas, llamadas paquetes, que el protocolo pueda manejar.
- Añade información de direccionamiento a los paquetes para que el ordenador de destino en la red pueda saber que el dato le pertenece.
- Prepara el dato para la transmisión actual a través de la tarjeta de red y fuera, por el cable.

### **2.3.2 El ordenador receptor**

En el ordenador receptor, un protocolo lleva a cabo la misma serie de pasos en orden inverso.

El ordenador receptor:

- Retira los datos del cable.
- Introduce los paquetes de datos en el ordenador a través de la tarjeta de red.
- Limpia los paquetes de datos, de toda la información de transmisión añadida Por el ordenador emisor.
- Copia el dato desde los paquetes a un buffer para reensamblarlos.
- Pasa los datos reensamblados a la aplicación en una forma utilizable.

Ambos, el emisor y el receptor necesitan realizar cada paso de la misma forma para que el dato parezca el mismo cuando se recibe que cuando se envió.

Por ejemplo, dos protocolos podrían romper el dato en paquetes y añadir información varia de secuencia, “Timing” y chequeo de error, pero cada uno lo podría hacer de diferente forma. Por lo tanto, un ordenador usando uno de esos protocolos no sería capaz de comunicarse con éxito con un ordenador utilizando el otro protocolo.

## **2.4 PROTOCOLOS EN UNA ARQUITECTURA EN NIVELES**

En una red, tienen que trabajar juntos varios protocolos para asegurar que el dato está:

- Preparado
- Transferido
- Recibido
- Manejado

El trabajo de los distintos protocolos debe estar coordinado para que no haya conflictos u operaciones incompletas. La respuesta a este esfuerzo de coordinación se llama “layering”.

### **2.4.1 Stacks de protocolos**

Un stack de protocolos es una combinación de protocolos. Cada nivel especifica un protocolo diferente para manejar una función o subsistema del proceso de comunicación. Cada nivel tiene su propio conjunto de reglas.

## **2.5 PROPIEDADES TÍPICAS DE LOS PROTOCOLOS**

Si bien los protocolos pueden variar mucho en propósito y sofisticación, la mayoría especifica una o más de las siguientes propiedades:

- Detección de la conexión física subyacente (con cable o inalámbrica), o la existencia de otro punto final o nodo.
- Handshaking.
- Negociación de varias características de la conexión.
- Cómo iniciar y finalizar un mensaje.
- Procedimientos en el formateo de un mensaje.
- Qué hacer con mensajes corruptos o formateados incorrectamente (corrección de errores).
- Cómo detectar una pérdida inesperada de la conexión, y qué hacer entonces.

- Terminación de la sesión y/o conexión.

Las características más importantes de un protocolo son:

- Directo/indirecto: los enlaces punto a punto son directos pero los enlaces entre dos entidades en diferentes redes son indirectos ya que intervienen elementos intermedios.
- Monolítico/estructurado: monolítico es aquel en que el emisor tiene el control en una sola capa de todo el proceso de transferencia. En protocolos estructurados, hay varias capas que se coordinan y que dividen la tarea de comunicación.
- Simétrico/asimétrico: los simétricos son aquellos en que las dos entidades que se comunican son semejantes en cuanto a poder tanto emisores como consumidores de información. Un protocolo es asimétrico si una de las entidades tiene funciones diferentes de la otra (por ejemplo en clientes y servidores).
- Normalizado/no normalizado: los no normalizados son aquellos creados específicamente para un caso concreto y que no va a ser necesario conectarlos con agentes externos. En la actualidad, para poder intercomunicar muchas entidades es necesaria una normalización.

## **2.6 FUNCIONES DE LOS PROTOCOLOS**

### **1. Segmentación y ensamblado:**

Generalmente es necesario dividir los bloques de datos en unidades pequeñas e iguales en tamaño, y este proceso se le llama segmentación. El bloque básico de segmento en una cierta capa de un protocolo se le llama PDU (Unidad de datos de protocolo). La necesidad de la utilización de bloque es por:

- La red sólo admite la transmisión de bloques de un cierto tamaño.
- El control de errores es más eficiente para bloques pequeños.

- Para evitar monopolización de la red para una entidad, se emplean bloques pequeños y así una compartición de la red.
- Con bloques pequeños las necesidades de almacenamiento temporal son menores.

Hay ciertas desventajas en la utilización de segmentos:

- La información de control necesaria en cada bloque disminuye la eficiencia en la transmisión.
- Los receptores pueden necesitar interrupciones para recibir cada bloque, con lo que en bloques pequeños habrá más interrupciones.
- Cuantas más PDU, más tiempo de procesamiento.

## **2. Encapsulado:**

Se trata del proceso de adherir información de control al segmento de datos. Esta información de control es el direccionamiento del emisor/receptor, código de detección de errores y control de protocolo.

## **3. Control de conexión:**

Hay bloques de datos sólo de control y otros de datos y control. Cuando se utilizan datagramas, todos los bloques incluyen control y datos ya que cada PDU se trata como independiente. En circuitos virtuales hay bloques de control que son los encargados de establecer la conexión del circuito virtual. Hay protocolos más sencillos y otros más complejos, por lo que los protocolos de los emisores y receptores deben de ser compatibles al menos. Además de la fase de establecimiento de conexión (en circuitos virtuales) está la fase de transferencia y la de corte de conexión. Si se utilizan circuitos virtuales habrá que numerar los PDU y llevar un control en el emisor y en el receptor de los números.



#### **4. Entrega ordenada:**

El envío de PDU puede acarrear el problema de que si hay varios caminos posibles, lleguen al receptor PDU desordenados o repetidos, por lo que el receptor debe de tener un mecanismo para reordenar los PDU. Hay sistemas que tienen un mecanismo de numeración con módulo algún número; esto hace que el módulo sean lo suficientemente alto como para que sea imposible que haya dos segmentos en la red al mismo tiempo y con el mismo número.

#### **5. Control de flujo:**

Hay controles de flujo de parada y espera o de ventana deslizante. El control de flujo es necesario en varios protocolos o capas, ya que el problema de saturación del receptor se puede producir en cualquier capa del protocolo.

#### **6. Control de errores:**

Generalmente se utiliza un temporizador para retransmitir una trama una vez que no se ha recibido confirmación después de expirar el tiempo del temporizador. Cada capa de protocolo debe de tener su propio control de errores.

#### **7. Direccionamiento:**

Cada estación o dispositivo intermedio de almacenamiento debe tener una dirección única. A su vez, en cada terminal o sistema final puede haber varios agentes o programas que utilizan la red, por lo que cada uno de ellos tiene asociado un puerto.

Cada estación o terminal de una subred debe de tener una dirección de subred (generalmente en el nivel MAC).

Hay ocasiones en las que se usa un identificador de conexión; esto se hace así cuando dos estaciones establecen un circuito virtual y a esa conexión la numeran (con un identificador de conexión conocido por ambas). La utilización de este identificador simplifica los mecanismos de envío de datos ya que por ejemplo es más sencillo que el direccionamiento global.

Algunas veces se hace necesario que un emisor emita hacia varias entidades a la vez y para eso se les asigna un direccionamiento similar a todas.

## **8. Multiplexación:**

Es posible multiplexar las conexiones de una capa hacia otra, es decir que de una única conexión de una capa superior, se pueden establecer varias conexiones en una capa inferior (y al revés).

## **9. Servicios de transmisión:**

Los servicios que puede prestar un protocolo son:

- **Prioridad:** hay mensajes (los de control) que deben tener prioridad respecto a otros.
- **Grado de servicio:** hay datos que deben de retardarse y otros acelerarse (vídeo).
- **Seguridad.**

## **2.7 PROTOCOLOS MÁS IMPORTANTES**

Los protocolos más importantes son el TCP/IP, NetBeui y el IPX/SPX. A continuación se explicaran con detalle estos tres protocolos.

### **2.7.1 El protocolo TCP/IP**

(Transmission Control Protocol/Internet Protocol) es el protocolo usado en Internet (la red de redes) y también para las Intranets (las redes locales).

En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet.

En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos.

Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería.

El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa.

Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

### **Historia del protocolo TCP/IP**

La Familia de Protocolos de Internet fue el resultado del trabajo llevado a cabo por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA por sus siglas en inglés) a principios de los 70. Después de la construcción de la pionera ARPANET en 1969 DARPA comenzó a trabajar en un gran número de tecnologías de transmisión de datos.

En 1972, Robert E. Kahn fue contratado por la Oficina de Técnicas de Procesamiento de Información de DARPA, donde trabajó en la comunicación de paquetes por satélite y por ondas de radio, reconoció el importante valor de la comunicación de estas dos formas.

Para el verano de 1973, Kahn había conseguido una remodelación fundamental, donde las diferencias entre los protocolos de red se ocultaban usando un Protocolo de comunicaciones y además, la red dejaba de ser responsable de la fiabilidad de la comunicación, como pasaba en ARPANET, era el host el responsable.

Con el papel que realizaban las redes en el proceso de comunicación reducido al mínimo, se convirtió en una posibilidad real comunicar redes diferentes, sin importar las características que éstas tuvieran.

Hay un dicho popular sobre el protocolo TCP/IP, que fue el producto final desarrollado por Kahn, que dice que este protocolo acabará funcionando incluso entre "dos latas unidas por un cordón".

En 1975, se realizó la primera prueba de comunicación entre dos redes con protocolos TCP/IP entre la Universidad de Stanford y la University College de Londres (UCL). En 1977, se realizó otra prueba de comunicación con un protocolo TCP/IP entre tres redes distintas con ubicaciones en Estados Unidos, Reino Unido y Noruega. Varios prototipos diferentes de protocolos TCP/IP se desarrollaron en múltiples centros de investigación entre los años 1978 y 1983. La migración completa de la red ARPANET al protocolo TCP/IP concluyó oficialmente el día 1 de enero de 1983 cuando los protocolos fueron activados permanentemente.

En marzo de 1982, el Departamento de Defensa de los Estados Unidos declaró al protocolo TCP/IP el estándar para las comunicaciones entre redes militares. En 1985, el Centro de Administración de Internet (Internet Architecture Board IAB por sus siglas en inglés) organizó un Taller de Trabajo de tres días de duración, al que asistieron 250 comerciales promocionando así el protocolo lo que contribuyó a un incremento de su uso comercial.

### **Ventajas e inconvenientes**

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web.

Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que NetBEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.

El conjunto TCP/IP se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, como así también en redes pequeñas o domésticas, y hasta en teléfonos móviles.

## **TCP**

Transmission Control Protocol (en español Protocolo de Control de Transmisión) o TCP, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

## **Funciones de TCP**

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

Los servicios provistos por TCP corren en el anfitrión (host) de cualquiera de los extremos de una conexión, no en la red. Por lo tanto, TCP es un protocolo para manejar conexiones de extremo a extremo. Tales conexiones pueden existir a través de una serie de conexiones punto a punto, por lo que estas conexiones extremo-extremo son llamadas circuitos virtuales.

Las características del TCP son:

- Orientado a la conexión: dos computadoras establecen una conexión para intercambiar datos. Los sistemas de los extremos se sincronizan con el otro para manejar el flujo de paquetes y adaptarse a la congestión de la red.
- Operación Full-Duplex: una conexión TCP es un par de circuitos virtuales, cada uno en una dirección. Sólo los dos sistemas finales sincronizados pueden usar la conexión.
- Error Checking: es usado para verificar que los paquetes no estén corruptos.
- Acknowledgements: sobre recibo de uno o más paquetes, el receptor regresa un acknowledgement (reconocimiento) al transmisor indicando que recibió los paquetes. Si los paquetes no son notificados, el transmisor puede reenviar los paquetes o terminar la conexión si el transmisor cree que el receptor no está más en la conexión.
- Control de flujo: si el transmisor está desbordando el buffer del receptor por transmitir demasiado rápido, el receptor descarta paquetes. Los acknowledgement fallidos que llegan al transmisor le alertan para bajar la tasa de transferencia o dejar de transmitir.
- Servicio de recuperación de Paquetes: el receptor puede pedir la retransmisión de un paquete. Si el paquete no es notificado como recibido (ACK), el transmisor envía de nuevo el paquete.

Los servicios confiables de entrega de datos son críticos para aplicaciones tales como transferencias de archivos (FTP por ejemplo), servicios de bases de datos, proceso de transacciones y otras aplicaciones de misión crítica en las cuales la entrega de cada paquete debe ser garantizada.

Las aplicaciones envían flujos de bytes a la capa TCP para ser enviados a la red. TCP divide el flujo de bytes llegado de la aplicación en segmentos de tamaño apropiado (normalmente esta limitación viene impuesta por la unidad máxima de transferencia (MTU) del nivel de enlace de datos de la red a la que la entidad está asociada) y le añade sus cabeceras. Entonces, TCP pasa el segmento resultante a la capa IP, donde a través de la red, llega a la capa TCP de la entidad destino. TCP comprueba que ningún segmento se ha perdido dando a cada uno un número de secuencia, que es también usado para asegurarse de que los paquetes han llegado a la entidad destino en el orden correcto.

TCP devuelve un asentimiento por bytes que han sido recibidos correctamente; un temporizador en la entidad origen del envío causará un timeout si el asentimiento no es recibido en un tiempo razonable, y el (presuntamente desaparecido) paquete será entonces retransmitido.

TCP revisa que no haya bytes dañados durante el envío usando un checksum; es calculado por el emisor en cada paquete antes de ser enviado, y comprobado por el receptor.

### **Funcionamiento del protocolo en detalle**

Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión.

Para establecer la conexión se usa el procedimiento llamado negociación en tres pasos (3-way handshake). Una negociación en cuatro pasos (4-way handshake) es usada para la desconexión.

Durante el establecimiento de la conexión, algunos parámetros como el número de secuencia son configurados para asegurar la entrega ordenada de los datos y la robustez de la comunicación.



## **Establecimiento de la conexión (negociación en tres pasos)**

Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un socket en un determinado puerto tcp y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete SYN inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit RST activado, lo que significa el rechazo del intento de conexión. En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión.

Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (spoofing).

## **Transferencia de datos**

Durante la etapa de transferencia de datos, una serie de mecanismos claves determinan la fiabilidad y robustez del protocolo.

Entre ellos están incluidos el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes duplicados, checksums para detectar errores, y asentimientos y temporizadores para detectar pérdidas y retrasos.

Durante el establecimiento de conexión TCP, los números iniciales de secuencia son intercambiados entre las dos entidades TCP. Estos números de secuencia son usados para identificar los datos dentro del flujo de bytes, y poder identificar (y contar) los bytes de los datos de la aplicación.

Siempre hay un par de números de secuencia incluidos en todo segmento TCP, referidos al número de secuencia y al número de asentimiento. Un emisor TCP se refiere a su propio número de secuencia cuando habla de número de secuencia, mientras que con el número de asentimiento se refiere al número de secuencia del receptor. Para mantener la fiabilidad, un receptor asiente los segmentos TCP indicando que ha recibido una parte del flujo continuo de bytes. Una mejora de TCP, llamada asentimiento selectivo (SACK, Selective Acknowledgement) permite a un receptor TCP asentir los datos que se han recibido de tal forma que el remitente solo retransmita los segmentos de datos que faltan.

A través del uso de números de secuencia y asentimiento, TCP puede pasar los segmentos recibidos en el orden correcto dentro del flujo de bytes a la aplicación receptora. Los números de secuencia son de 32 bits (sin signo), que vuelve a cero tras el siguiente byte después del 2<sup>32</sup>-1. Una de las claves para mantener la robustez y la seguridad de las conexiones TCP es la selección del número inicial de secuencia (ISN, Initial Sequence Number).

Un checksum de 16 bits, consistente en el complemento a uno de la suma en complemento a uno del contenido de la cabecera y datos del segmento TCP, es calculado por el emisor, e incluido en la transmisión del segmento. Se usa la suma en complemento a uno porque el acarreo final de ese método puede ser calculado en cualquier múltiplo de su tamaño (16-bit, 32-bit, 64-bit...) y el resultado, una vez plegado, será el mismo. El receptor TCP recalcula el checksum sobre las cabeceras y datos recibidos. El complemento es usado para que el receptor no tenga que poner a cero el campo del checksum de la cabecera antes de hacer los cálculos, salvando en algún lugar el valor del checksum recibido; en vez de eso, el receptor simplemente calcula la suma en complemento a uno con el checksum incluido, y el resultado debe ser igual a 0. Si es así, se asume que el segmento ha llegado intacto y sin errores.

Hay que fijarse en que el checksum de TCP también cubre los 96 bit de la cabecera que contiene la dirección origen, la dirección destino, el protocolo y el tamaño TCP. Esto proporciona protección contra paquetes mal dirigidos por errores en las direcciones.

El checksum de TCP es una comprobación bastante débil. En niveles de enlace con una alta probabilidad de error de bit quizá requiera una capacidad adicional de corrección/detección de errores de enlace. Si TCP fuese rediseñado hoy, muy probablemente tendría un código de redundancia cíclica (CRC) para control de errores en vez del actual checksum.

La debilidad del checksum está parcialmente compensada por el extendido uso de un CRC en el nivel de enlace, bajo TCP e IP, como el usado en el PPP o en Ethernet.

Sin embargo, esto no significa que el checksum de 16 bits es redundante: sorprendentemente, inspecciones sobre el tráfico de Internet han mostrado que son comunes los errores de software y hardware[cita requerida] que introducen errores en los paquetes protegidos con un CRC, y que el checksum de 16 bits de TCP detecta la mayoría de estos errores simples.

Los asentimientos (ACKs o Acknowledgments) de los datos enviados o la falta de ellos, son usados por los emisores para interpretar las condiciones de la red entre el emisor y receptor TCP.

Unido a los temporizadores, los emisores y receptores TCP pueden alterar el comportamiento del movimiento de datos. TCP usa una serie de mecanismos para conseguir un alto rendimiento y evitar la congestión de la red (la idea es enviar tan rápido como el receptor pueda recibir). Estos mecanismos incluyen el uso de ventana deslizante, que controla que el transmisor mande información dentro de los límites del buffer del receptor, y algoritmos de control de flujo, tales como el algoritmo de Evitación de la Congestión (congestion avoidance), el de comienzo lento (Slow-start), el de retransmisión rápida, el de recuperación rápida (Fast Recovery), y otros.

## **Puertos TCP**

TCP usa el concepto de número de puerto para identificar a las aplicaciones emisoras y receptoras.

Cada lado de la conexión TCP tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora. Los puertos son clasificados en tres categorías: bien conocidos, registrados y dinámicos/privados. Los puertos bien conocidos son asignados por la Internet Assigned Numbers Authority (IANA), van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios.

Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones. Algunos ejemplos son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80). Los puertos registrados son normalmente empleados por las aplicaciones de usuario de forma temporal cuando conectan con los servidores, pero también pueden representar servicios que hayan sido registrados por un tercero (rango de puertos registrados: 1024 al 49151). Los puertos dinámicos/privados también pueden ser usados por las aplicaciones de usuario, pero este caso es menos común. Los puertos dinámicos/privados no tienen significado fuera de la conexión TCP en la que fueron usados (rango de puertos dinámicos/privados: 49152 al 65535, recordemos que el rango total de 2 elevado a la potencia 16, cubre 65536 números, del 0 al 65535).

### **2.7.2 IP**

Internet Protocol (en español Protocolo de Internet) o IP es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco).

IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (switches) y los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits (lo cual asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670.000 millones de direcciones IP), muchas más direcciones que las que provee IPv4 con 32 bits.

Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

## **Direccionamiento IP y enrutamiento**

Quizás los aspectos más complejos de IP son el direccionamiento y el enrutamiento. El direccionamiento se refiere a la forma como se asigna una dirección IP y como se dividen y se agrupan subredes de equipos.

El enrutamiento consiste en encontrar un camino que conecte una red con otra y, aunque es llevado a cabo por todos los equipos, es realizado principalmente por enrutadores, que no son más que computadores especializados en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos.

## **Dirección IP**

Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo de Internet (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar, y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática); es decir, no cambia con el tiempo. Los servidores de correo, dns, ftp públicos, servidores web, necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación.

Las máquinas tienen una gran facilidad para manipular y jerarquizar la información numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP. Sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar; tal es el caso URLs y resolución de nombres de dominio DNS.

Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

## **Enrutamiento**

En comunicaciones, el encaminamiento (a veces conocido por el anglicismo ruteo o enrutamiento) es el mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Asociado al encaminamiento existe el concepto de métrica, que es una medida de lo "bueno" que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, coste, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Si la métrica es el retardo, es mejor un camino cuyo retardo total sea menor que el de otro. Lo ideal en una red es conseguir el encaminamiento óptimo: tener caminos de distancia (o coste, o retardo, o la magnitud que sea, según la métrica) mínimos. Típicamente el encaminamiento es una función implantada en la capa 3 (capa de red) del modelo de referencia OSI.

### **2.7.3 El protocolo NETBEUI**

NetBEUI (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sin encaminamiento y bastante sencillo utilizado como una de las capas en las primeras redes de Microsoft.

NetBIOS sobre NetBEUI es utilizado por muchos sistemas operativos desarrollados en los 1990, como LAN Manager, LAN Server, Windows 3.x, Windows 95 y Windows NT.

Este protocolo a veces es confundido con NetBIOS, pero NetBIOS es una idea de cómo un grupo de servicios deben ser dados a las aplicaciones. Con NetBEUI se convierte en un protocolo que implementa estos servicios. NetBEUI puede ser visto como una implementación de NetBIOS sobre IEEE 802.2 LLC. Otros protocolos, como NetBIOS sobre IPX/SPX o NetBIOS sobre TCP/IP, también implementan los servicios de NetBIOS pero con sus propias herramientas.

NetBEUI usa el modo 1 de IEEE 802.2 para proveer el servicio de nombres y el de datagramas, y el modo 2 para proveer el servicio de sesión. NetBEUI abusa de los mensajes broadcast, por lo que se ganó la reputación de usar la interfaz en exceso.

NetBIOS fue desarrollada para las redes de IBM por Saytek, y lo uso también Microsoft en su MS-NET en 1985. En 1987 Microsoft y Novell usaron también este protocolo para su red de los sistemas operativos LAN Manager y NetWare.

Debido a que NetBEUI no tiene encaminamiento, sólo puede usarse para comunicar terminales en el mismo segmento de red, pero puede comunicar dos segmentos de red que estén conectados mediante un puente de red.

Esto significa que sólo es recomendable para redes medianas o pequeñas. Para poder usar este protocolo en redes más grandes de forma óptima debe ser implementado sobre otros protocolos como IPX o TCP/IP.

El NetBeui es utilizado de forma general en redes con PC's que tienen instalado algún sistema operativo Microsoft.

## **Servicios**

NetBeui da tres servicios:

- Servicio de nombres, para registro y resolución de nombres



- Servicio de sesión para comunicaciones con la conexión
- Servicio de distribución de datagramas para comunicaciones sin conexión

### **Servicio de nombres**

Para comenzar una sesión o distribuir datagramas, una aplicación tiene que registrar su nombre en la red usando el servicio de nombres de la NetBIOS. Para esto, se distribuye a toda la red un paquete broadcast con la petición para añadir su nombre (Add Name Query), o para incluirse en un nombre de grupo (Add Group Name Query). Si el nombre que quería usar en la red está en uso, el servicio de nombres de la máquina que lo tiene en ese momento lanza un mensaje broadcast indicando un conflicto de nodos (Node conflict).

Para comenzar una sesión o para enviar un datagrama a una máquina en concreto, en vez de mandar el datagrama por broadcast a toda la red, NetBEUI determina la dirección MAC de la máquina con su nombre de red. Este proceso se hace enviando un paquete de petición de nombre (Name Query), cuya respuesta tendrá la dirección MAC de la máquina que envía dicha respuesta, es decir la MAC.

### **Servicio de sesión**

El servicio de sesión permite que dos terminales de la red establezcan una conexión, permitiendo el envío y recepción de mensajes de mayor tamaño. También da un servicio de detección de errores y de recuperación de los mismos.

Las sesiones se establecen mediante el intercambio de paquetes. La máquina que va a establecer la sesión envía una petición de nombre (Name Query) especificando que desea iniciar una sesión. La máquina con la que se va a establecer la sesión enviará una respuesta de nombre reconocido (Name Recognized), indicando tanto que no se puede establecer una sesión (debido a que el terminal no acepta sesiones para ese nombre, que no tiene recursos, etc.), como que se puede establecer (en cuyo caso la respuesta incluirá un número de sesión para usar en los subpaquetes).

La máquina que comenzó la sesión enviará una petición de sesión inicializada (Sesión Initialize), que a su vez provocará una respuesta de sesión confirmada (Sesión Confirm).

Los datos son transmitidos durante una conexión establecida. Debido a que NetBIOS permite que los paquetes enviados sean mayores que el tamaño máximo establecido en otras capas, un paquete NetBIOS debe ser transmitido como una secuencia de paquetes intermediarios (Data First Middle), y un paquete final (Data Only Last). Los paquetes que no necesitan ser segmentados de esta forma se envían siempre como un paquete final. Los paquetes finales recibidos de forma correcta, provocan el envío de una señal de acuse de recibo (ACK o acknowledgment). En el caso de haber paquetes intermedios, el acuse de recibo también confirma todos los enviados. La sesión se cierra enviando una petición de final de sesión (Sesión End).

### **Servicio de distribución de datagramas**

El servicio de envío de datagramas es sin conexión. Los datagramas se envían como paquetes de tipo datagrama si se van a enviar a un nombre NetBIOS concreto, o como paquetes tipo datagramas broadcast si van a ser enviados a toda la red.

NetBEUI es oficialmente soportado por Microsoft en todos sus sistemas operativos hasta Windows 2000, pero su uso va rápidamente en descenso desde la aparición de NetBIOS sobre TCP/IP.

### **2.7.4 El protocolo IPX/SPX**

Es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare. Algunos de los juegos en red y "on line" solo pueden disfrutarse si se tiene instalado.

## **Historia**

Creados a principios de 1988, deriva de la familia de protocolos Xerox Network Services (XNS) de Xerox y fueron diseñados para eliminar la necesidad de enumerar los nodos individuales de una red. En un principio fueron propietarios, aunque más adelante se han implementado en otros sistemas operativos (como por ejemplo el NWLink en el caso de Windows).

Ha sobrevivido durante aproximadamente unos 15 años ya que actualmente está en desuso desde que el boom de Internet hizo a TCP/IP casi universal. Una de las diversas razones de su desuso es que como los ordenadores y las redes actuales pueden utilizar múltiples protocolos de red, casi todos los sitios con IPX usarán también TCP/IP para permitir la conectividad con Internet.

En versiones recientes del NetWare (a partir de la 5) ya se ha reemplazado al IPX por el TCP/IP, aunque sigue siendo posible su uso. En la actualidad su uso se ha reducido únicamente a juegos en red antiguos.

## **Protocolos que lo componen**

### **IPX**

El protocolo Intercambio de Paquetes Entre Redes (IPX) es la implementación del protocolo IDP (Internet Datagram Protocol) de Xerox. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

Pertenece a la capa de red (nivel 3 del modelo OSI) y al ser un protocolo de datagramas es similar (aunque más simple y con menor fiabilidad) al protocolo IP del TCP/IP en sus operaciones básicas pero diferente en cuanto al sistema de direccionamiento, formato de los paquetes y el ámbito general. Fue creado por Alexis G.Soulle.

## **SPX**

El protocolo Intercambio de Paquetes en Secuencia (SPX) es la implementación del protocolo SPP (Sequenced Packet Protocol) de Xerox. Es un protocolo fiable basado en comunicaciones con conexión y se encarga de controlar la integridad de los paquetes y confirmar los paquetes recibidos a través de una red.

Pertenece a la capa de transporte (nivel 4 del modelo OSI) y actúa sobre IPX para asegurar la entrega de los paquetes (datos), ya que IPX por sí solo no es capaz. Es similar a TCP ya que realiza las mismas funciones. Se utiliza principalmente para aplicaciones cliente/servidor.

### **Direccionamiento**

Soporta direcciones de 32 bits que se asignan completamente sobre una red en vez de sobre equipos individuales. Para identificar cada equipo dentro de la red, se emplea hardware específico.

Cada dirección posee tres componentes:

1. Dirección de red, valor de 32 bits asignado por un administrador y limitado a una determinada red.
2. Número del nodo, derivada de una dirección MAC de 48 bits que es obtenida por una tarjeta de red.
3. Número de socket, valor de 16 bits asignado por el sistema operativo de red (p.e NetWare) a un proceso específico dentro de un nodo.

### **Ventajas e inconvenientes**

Se ha utilizado sobre todo en redes de área local (LAN) porque es muy eficiente para este propósito (típicamente su rendimiento supera al de TCP/IP en una LAN).

Los inconvenientes que presentan es que en redes metropolitanas (MANs) y grandes (WANs) no se puede enrutar y por tanto no es utilizable, y también puede llegar a saturar la red con el alto nivel de tráfico que genera los broadcast que lanzan los equipos para anunciarse en la red.

## **2.8 UN MODELO DE TRES CAPAS**

En la comunicación intervienen tres agentes: aplicaciones, computadores y redes.

Por lo tanto, es lógico organizar la tarea en tres capas.

1. Capa de acceso a la red: Trata del intercambio de datos entre el computador y la red a que está conectado.
2. Capa de transporte: consiste en una serie de procedimientos comunes a todas las aplicaciones que controlen y sincronicen el acceso a la capa de acceso a la red.
3. Capa de aplicación: permite la utilización a la vez de varias aplicaciones de usuario.

El protocolo debe definir las reglas, convenios, funciones utilizadas, etc. Para la comunicación por medio de red.

Cada capa del protocolo le pasa datos a la siguiente capa y ésta le añade datos propios de control y luego pasa el conjunto a la siguiente capa. Por tanto, cada capa forma unidades de datos que contienen los datos tomados de la capa anterior junto a datos propios de esta capa, y al conjunto obtenido se le llama PDU (unidad de datos del protocolo).

## 2.9 PROTOCOLOS RUTEABLES VS NO RUTEABLES

Hasta mediados los 80, la mayoría de las redes están aisladas. Servían a un departamento único o compañía y se conectaban raramente a otros entornos más grandes.

Así, cuando maduró la tecnología de LAN y las necesidades de comunicaciones de datos en los negocios crecían, las LAN llegaron a ser componentes de grandes redes de comunicación de datos donde las redes hablaban entre sí.

Los datos eran enviados desde una LAN a otra a través de varios caminos disponibles son enrutados.

Los protocolos que soportan comunicaciones “LAN-to-LAN multipath” son conocidos como protocolos ruteables. Dado que los protocolos ruteables pueden usarse para enlazar juntas varias LAN y crear nuevos entornos de amplia área, están incrementando su importancia.

Para comunicar redes distintas hace falta enrutamiento.

En éste capítulo pudimos ver lo que significa un protocolo y la importancia de éste en las redes de computadora además de conocer los protocolos más importantes y su definición, es así como termina este segundo capítulo para dar paso a los siguientes temas que tratarán de las diferentes topologías de red, métodos de acceso y medios de transmisión.

## CAPITULO III

### TOPOLOGÍAS DE RED, MÉTODOS DE ACCESO Y MEDIOS DE TRANSMISIÓN

En este capítulo abordaremos tres temas de gran importancia en las redes de computadoras empezando por la definición de lo que es una topología de red y los diferentes tipos que podemos encontrar, después mencionaremos los métodos de acceso que se utilizan para definir la forma en que se colocan los datos en la red y por último haremos mención de los medios de transmisión en las redes de computadoras.

#### 3.1 Topologías de Red

Según el libro titulado Redes de Computadoras escrito por Andrew S. Tanenbaum, Prentice Hall, 3ª edición, se define una topología de red de la siguiente manera:

“La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada.

La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí.”

Por lo tanto, la topología establece la forma en cuanto a conectividad física de la red. El término topología se utiliza en geometría para describir la forma de un objeto. El diseñador de una red tiene tres objetivos al establecer la topología de la misma y son los siguientes:

- Proporcionar la máxima fiabilidad a la hora de establecer el tráfico
- Encaminar el tráfico utilizando la vía de costo mínimo (aunque a veces no se escoge la vía de costo mínimo porque otros factores, como la fiabilidad, pueden ser más importantes)

- Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo

Las topologías de red más comunes son:

- La topología jerárquica (en árbol)
- La topología horizontal (en bus)
- La topología en estrella
- La topología en anillo
- La topología en malla

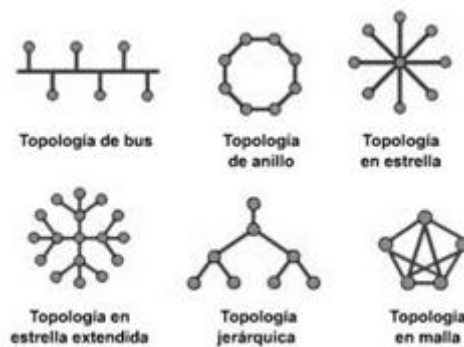


Fig. 2

### Topologías Físicas

#### 3.1.1 Topología Jerárquica (en árbol).

Es llamada así por su apariencia estética, por la cual puede comenzar con la inserción del servicio de internet desde el proveedor, pasando por el router, luego por un switch y este deriva a otro switch u otro router o sencillamente a los hosts (estaciones de trabajo).



El resultado de esto es una red con apariencia de árbol porque desde el primer router que se tiene se ramifica la distribución de internet dando lugar a la creación de nuevas redes o subredes tanto internas como externas.

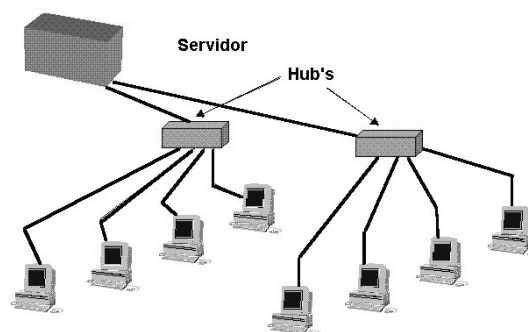


Fig. 3  
Topología de árbol

La topología jerárquica es una de las más comúnmente utilizadas hoy en día. El software para controlar la red es relativamente simple y la propia topología proporciona un punto de concentración para control y resolución de errores.

Aunque la topología jerárquica es atractiva desde el punto de vista de la simplicidad de control, presenta problemas serios de cuellos de botella. El problema no son sólo los cuellos de botella, sino también la fiabilidad. En el caso de un fallo en la máquina situada en la raíz, la red queda completamente fuera de servicio, a no ser que otro nodo asuma las funciones del nodo averiado. Permite una evolución simple hacia redes más complejas, ya que es muy sencillo añadir nuevos componentes.

### 3.1.2 Topología Horizontal (en bus).

Permite que todas las computadoras conectadas en red, llamadas estaciones de trabajo o terminales, reciban todas las transmisiones.

La desventaja de esta topología está en el hecho de que suele existir un solo canal de comunicación para todos los dispositivos de la red. En consecuencia si falla un tramo de la red, toda la red deja de funcionar.

Esta topología se recomienda cuando la red de datos a implementar es menor o igual a cuatro estaciones de trabajo además de tener poca seguridad.

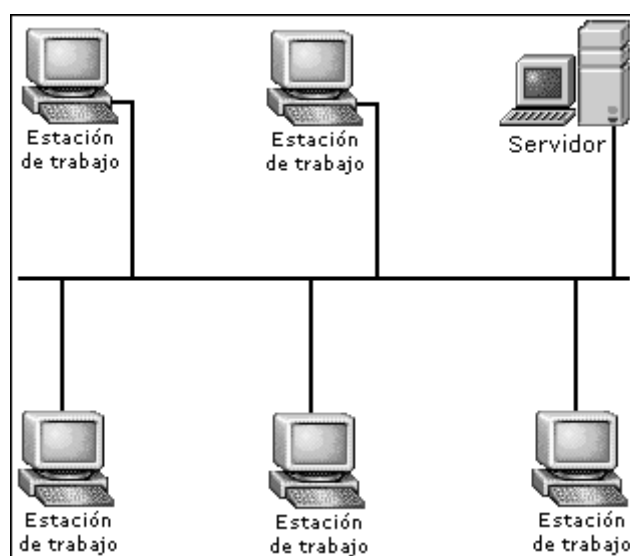


Fig. 4  
Topología de bus

Algunos fabricantes suministran un canal redundante que se pone en funcionamiento en el caso de fallo en el canal primero. En otros casos se proporcionan procedimientos para evitar los nodos que fallen.

Otro problema que presenta esta configuración es la dificultad de aislar los componentes defectuosos conectados al bus, debido a la ausencia de puntos de concentración.

### 3.1.3 Topología en Estrella

Es otra estructura ampliamente usada en sistemas de comunicación de datos. Una de las principales razones para su uso es fundamentalmente histórica. Todo el tráfico surge del centro de la estrella.

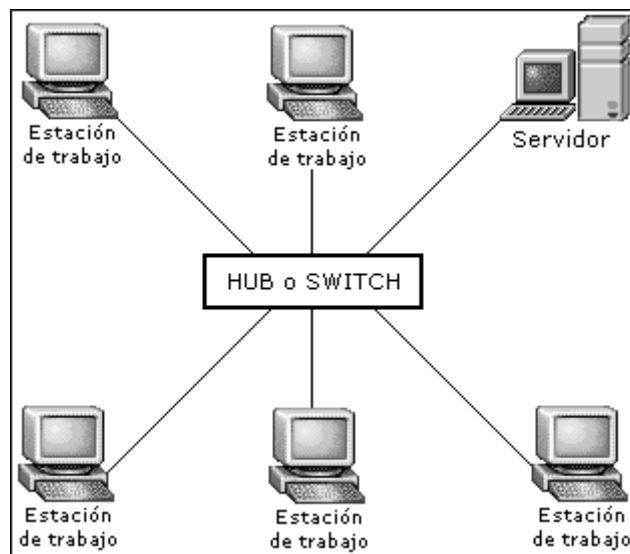


Fig. 5  
Topología en Estrella

Por lo tanto es una estructura muy semejante a la estructura jerárquica, con la diferencia de que la estructura en estrella tiene mucho más limitadas las posibilidades de procesamiento distribuido.

La localización de averías es relativamente simple en redes en estrella ya que es posible ir aislando las líneas para identificar el problema. Sin embargo, como sucedía en la estructura jerárquica, la red en estrella sufre de los mismos problemas de fallos y cuellos de botella, debido al nodo central.

Algunos sistemas poseen un nodo central de reserva, lo que incrementa considerablemente la confiabilidad del sistema.

### 3.1.4 Topología en Anillo

Este tipo de topología recibe su nombre del aspecto circular del flujo de datos. En muchos casos el flujo de datos va en una sola dirección, es decir, una estación recibe la señal y la envía a la siguiente estación del anillo. La lógica necesaria en una red de este tipo es relativamente simple.

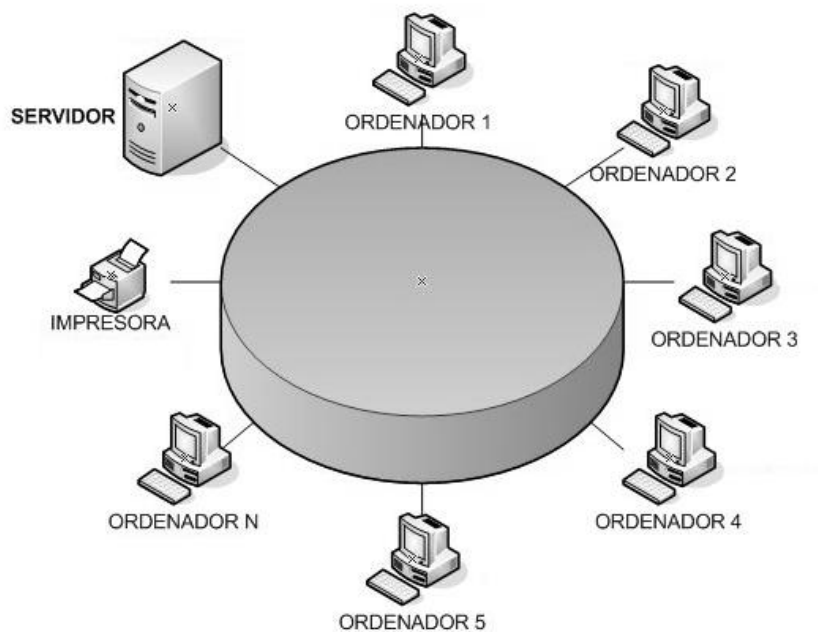


Fig. 6  
Topología en anillo

Como todas las redes, el anillo tiene también sus inconvenientes. El principal de ellos es que un único canal une a todos los componentes del anillo. Si falla el canal entre dos nodos, falla toda la red. En consecuencia algunos sistemas incorporan canales de reserva.

En otros casos se proporciona la posibilidad de evitar el enlace defectuoso, de forma que la red no quede fuera de servicio.

### 3.1.5 Topología en Malla

La topología en malla es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones.

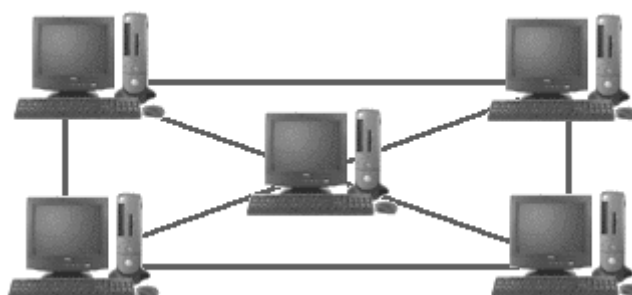


Fig. 7

Red en Malla

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que los elementos de la red (nodo) están conectados todos con todos, mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red de modo que, si falla un cable, otro se hará cargo del tráfico.

Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).

Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado.

### 3.1.6 Variaciones en las principales topologías

Hoy, muchas topologías que están trabajando, son combinaciones del bus, la estrella, y el anillo.

En el libro Fundamentos de Redes Plus, Microsoft Corporation, Mc Graw Hill, se hace mención de las siguientes variaciones en las topologías de red.

#### Bus en Estrella.

El bus en estrella es una combinación de las topologías de bus y de estrella. En una topología de bus en estrella hay varias redes con topología en estrella conectadas juntas con troncales de bus líneas.

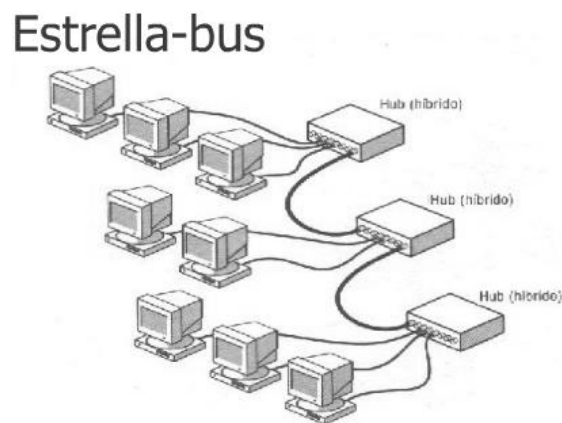


Fig.8

Estrella-bus

Si un ordenador, cae, no afectará al resto de la red. Los otros serán capaces de comunicarse. Si un hub cae, todos los ordenadores en ese hub son incapaces de comunicarse. Si un hub está conectado a otros hubs, esas conexiones también estarán rotas.

## Anillo en Estrella

El anillo en estrella, es similar al bus en estrella. Ambas, el anillo en estrella, y el bus en estrella, están centradas en un hub que contiene el anillo actual o el bus. Los hubs en un bus en estrella están conectados por troncales de bus lineales, mientras que los hubs en un anillo en estrella están conectados en un modelo de estrella por el hub principal.

### Estrella-Anillo

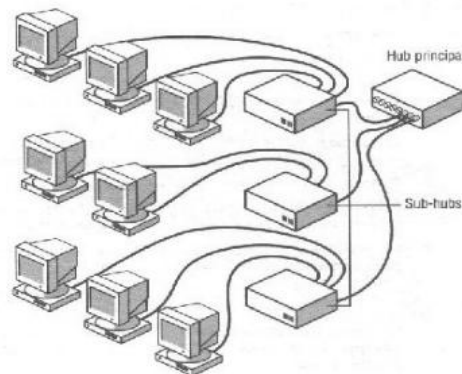


Fig. 9

Estrella-Anillo

Además de estas variaciones el libro maneja las siguientes ventajas y desventajas del uso de las topologías de red.

### Ventajas y desventajas de las topologías.

Hay varios factores a considerar cuando se determina qué topología cubre las necesidades de una organización.

### Bus

Ventajas:

- Económico uso del cable.
- El cable es barato y fácil de trabajar.
- Simple, segura.

- Fácil de extender.

Desventajas:

- La red puede caer con tráfico fuerte.
- Los problemas son difíciles de aislar.
- La rotura del cable puede afectar a muchos usuarios.

## **Anillo**

Ventajas:

- Acceso igual para todos los ordenadores.
- Prestaciones uniformes a pesar de la existencia de muchos usuarios.

Desventajas:

- El fallo de un ordenador puede impactar al resto de la red.
- Problemas difíciles de aislar.
- La reconfiguración de la red interrumpe las operaciones.

## **Estrella y Árbol**

Ventajas:

- Fácil de modificar y añadir nuevos ordenadores.
- Monitorización y manejo centralizado.
- El fallo de un ordenador no afecta al resto de la red.

Desventajas:

- Si el punto centralizado falla, la red falla.



## **Malla**

Ventajas:

- El fallo de un equipo no afecta el resto de la red
- El sistema ofrece un incremento de la redundancia y la fiabilidad, así como facilidad para resolver problemas

Desventajas:

- El sistema es caro de instalar ya que utiliza mucho cableado

### **3.2 MÉTODOS DE ACCESO**

Se denomina método de acceso al conjunto de reglas que definen la forma en que un equipo coloca los datos en la red y toma los datos del cable. Una vez que los datos se están moviendo en la red, los métodos de acceso ayudan a regular el flujo del tráfico de la red.

Una red es de alguna forma como la vía de un tren, por la que circulan varios trenes. Además de la vía, suele haber estaciones de tren. Cuando un tren está en la vía, el resto de los trenes deben respetar un procedimiento que gobierna cómo y cuándo entran en el flujo de tráfico. Sin dicho procedimiento, la entrada de un tren podría colisionar con otro que ya estuviese en la vía.

Sin embargo, hay diferencias importantes entre un sistema de vías de tren y una red de equipos. En una red, parece que todo el tráfico se mueve simultáneamente, sin interrupción. No obstante, esta apariencia es una ilusión; en realidad, los equipos toman turnos para acceder a la red durante breves períodos de tiempo. La mayor diferencia está en la mayor velocidad en la que se mueve el tráfico de la red.

Si los equipos utilizan métodos de acceso distintos, la red podría tener problemas, debido a que unos métodos podrían dominar el cable.

### **3.2.1 Clasificación métodos de acceso**

En el libro Tecnologías de Interconectividad de Redes, Merilee Ford, H. Kim Lew, Prentice Hall, CISCO Systems. se hace mención de la siguiente clasificación.

“Hay dos métodos de acceso de uso generalizado en redes locales: el acceso por contención, llamado también acceso aleatorio y el acceso determinístico.

Básicamente, el método de acceso por contención permite que cualquier usuario empiece a transmitir en cualquier momento siempre que el camino o medio físico no esté ocupado. En el método determinístico, cada estación tiene asegurada su oportunidad de transmitir siguiendo un criterio rotatorio.”

#### **1. Acceso por contención, aleatorio o no determinístico.**

Los métodos aleatorios o por contención utilizan redes con topología en bus; su señal se propaga por toda la red y llega a todos los ordenadores. Este sistema de enviar la señal se conoce como broadcast.

El método de contención más común es el CSMA (Carrier Sense Multiple Access) o traducido al español Acceso Múltiple Sensor de Portadora.

Opera bajo el principio de escuchar antes de hablar, de manera similar a la radio de los taxis. El método CSMA está diseñado para redes que comparten el medio de transmisión.

Cuando una estación quiere enviar datos, primero escucha el canal para ver si alguien está transmitiendo. Si la línea está desocupada, la estación transmite. Si está ocupada, espera hasta que esté libre.

Cuando dos estaciones transmiten al mismo tiempo habrá, lógicamente, una colisión. Para solucionar este problema existen dos técnicas diferentes, que son dos tipos de protocolos CSMA: uno es llamado CA (Collision Avoidance), en español, Prevención de Colisión y el otro CD (Collision Detection) en español Detección de Colisión. La diferencia entre estos dos enfoques se reduce al envío o no envío de una señal de agradecimiento por parte del nodo receptor:

**Collision Avoidance (CA):** Es un proceso en tres fases en las que el emisor:

1. Escucha para ver si la red está libre
2. Transmite el dato
3. Espera un reconocimiento por parte del receptor

Este método asegura así que el mensaje se recibe correctamente. Sin embargo, debido a las dos transmisiones, la del mensaje original y la del reconocimiento del receptor, pierde un poco de eficiencia.

**Collision Detection (CD):** Después de transmitir, el emisor escucha si se produce una colisión. Si no oye nada asume que el mensaje fue recibido. Aunque al no haber reconocimiento, no hay garantía de que el mensaje se haya recibido correctamente. Cuando varias personas mantienen una conversación, puede haber momentos en los que hablen a la vez dos o más personas. La que intenta comunicar, al detectar que su conversación ha colisionado con otra, debe iniciar de nuevo la conversación.

Si dos estaciones inician la transmisión simultáneamente se produce una colisión de las señales. La estación emisora, cuando detecta la colisión, bloquea la red para asegurar que todas las estaciones involucradas procesan el envío como erróneo.

Entonces, cada estación espera un periodo corto de tiempo fijado aleatoriamente, antes de intentar transmitir de nuevo.

Aunque estos métodos puedan parecer imprecisos son de hecho muy exactos. Bajo condiciones de carga normales, raras veces ocurren colisiones y cuando aparecen, el emisor lo reintentará hasta que envíe su mensaje.

## **2. Acceso determinístico.**

El segundo de los métodos más usados es el de acceso determinístico. El sistema determina qué estación es la que puede transmitir en cada instante de tiempo.

El método determinístico más usado es el Token Passing o paso de testigo. En una red Token Passing una secuencia especial de bits, el testigo, recorre la red de una estación a otra siguiendo un orden predeterminado. Cuando una estación quiere transmitir, espera que le llegue el testigo y lo guarda; envía su mensaje que circula por toda la red hasta volver a la estación emisora, entonces libera el testigo que viaja hasta la siguiente estación de red.

Los sistemas Token Passing están diseñados para resistir fuertes cargas de trabajo. Al ser un sistema ordenado, una red local usando el método Token Passing puede aprovechar el ancho de banda de trabajo hasta en un 90%. En principio, en un sistema con mucho tráfico, los retardos son menores usando métodos de acceso determinístico (Token Passing) que por contención (CSMA/CA-CD). Sin embargo, en un sistema sin mucha carga el método de contención es bastante rápido y eficaz.

Uno de los factores más importantes que se deben tener en cuenta para evaluar el comportamiento de una red es el número de estaciones. En las redes con acceso determinístico el token (testigo) circula a través de la red, teniendo cada estación derecho a transmitir antes de que se inicie una segunda vuelta. En una red de acceso por contención (aleatorio) el factor crítico será la carga de la red. La degradación del rendimiento es más predecible en una red Token Passing que en una CSMA/CD.

Algunos ejemplos de redes de acceso determinístico son la TokenRing de IBM y la Arcnet de Datapoint.

La posibilidad de detección de colisiones es el parámetro que impone una limitación en cuanto a distancia en CSMA/CD. Debido a la atenuación, el debilitamiento de una señal transmitida a medida que se aleja del origen, el mecanismo de detección de colisiones no es apropiado a partir de 2.500 metros (1.5 millas).

Los segmentos no pueden detectar señales a partir de esa distancia y, por tanto, no se puede asegurar que un equipo del otro extremo esté transmitiendo. Si más de un equipo transmite datos en la red al mismo tiempo, se producirá una colisión de datos y los datos se estropearán.

### **3.3 MEDIOS DE TRANSMISION.**

El medio de transmisión consiste en el elemento que conecta físicamente las estaciones de trabajo al servidor y los recursos de la red. Entre los diferentes medios utilizados en las LANs se puede mencionar: el cable de par trenzado, el cable coaxial, la fibra óptica y el espectro electromagnético (en transmisiones inalámbricas).

Su uso depende del tipo de aplicación particular ya que cada medio tiene sus propias características de costo, facilidad de instalación, ancho de banda soportado y velocidades de transmisión máxima permitidas.

#### **3.3.1 Principales tipos de cables**

La inmensa mayoría de las redes de hoy en día están conectadas por algún tipo de malla o cableado, que actúa como el medio de transmisión en la red, transportando señales entre ordenadores. Hay una variedad de cables que pueden cubrir las necesidades y los distintos tamaños de las redes, desde pequeñas a grandes.

Afortunadamente, solo tres principales grupos de cables conectan la mayoría de las redes:

- Coaxial.

- Par Trenzado
  - Par trenzado sin blindar (UTP)
  - Par trenzado blindado (STP)
  
- Fibra óptica.

### **3.3.2 Cable Coaxial**

En un momento dado, el cable coaxial fue el cable de red más ampliamente utilizado. Había un par de razones para el amplio uso del coaxial.

El coaxial era relativamente barato, ligero, flexible y fácil de trabajar con él. Era tan popular que llegó a ser un medio seguro y fácil de soportar en una instalación.

En la forma más simple, el coaxial consiste en un núcleo hecho de cobre sólido envuelto por un aislamiento, un trenzado de metal escudándolo y una capa exterior.

Una capa de película metálica y otra capa de trenzado de metal escudando se conoce como un doble aislamiento. Sin embargo, hay disponible un aislamiento de calidad para entornos sujetos a fuertes interferencias. El aislamiento de calidad consiste en dos capas de película metálica y dos capas de malla metálica.

El aislamiento se refiere al entretejido o malla de metal trenzado que rodea algunos tipos de cable.

El aislamiento protege los datos transmitidos absorbiendo señales electrónicas dispersas, llamadas “ruido”, para que no entren en el cable y distorsionen los datos.

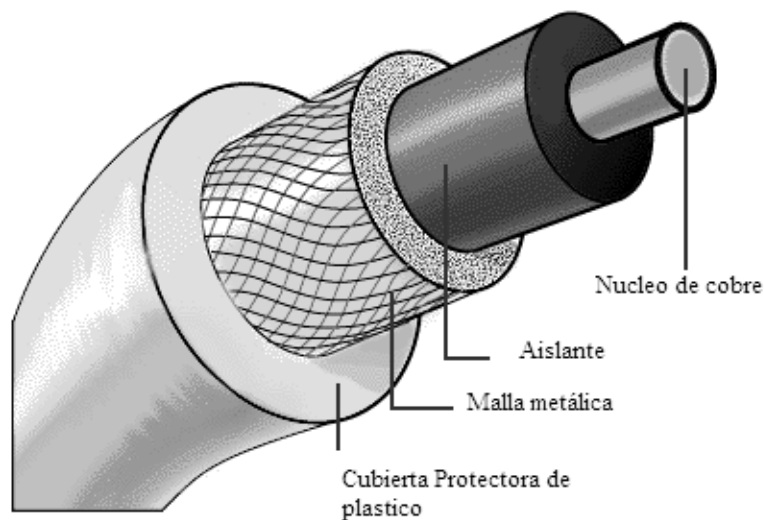


Fig. 10  
Cable Coaxial

El núcleo del cable coaxial transporta las señales electrónicas que conforman los datos. Este hilo del núcleo puede ser sólido o trenzado. Si el núcleo es sólido, usualmente es cobre.

El núcleo está envuelto por una capa de aislamiento que le separa de la malla. La malla trenzada actúa como tierra y protege el núcleo de ruido eléctrico y réplicas (Crosstalk). Las réplicas son desbordamientos de señal desde un cable cercano.

El núcleo conductor y la malla deben estar siempre separados el uno del otro. Si se tocan, el cable experimentará un corto, y fluirán ruido o señales dispersas en la malla, en el hilo de cobre. Esto podría destruir los datos.

El cable entero está rodeado por una capa no conductora, usualmente hecha de caucho, Teflón o plástico.

El cable coaxial es más resistente a interferencias y atenuación que el cable de par trenzado. Atenuación es la pérdida de fuerza en la señal, que empieza a ocurrir en cuanto la señal viaja a través del cable de cobre.

El trenzado, es como un manguito protector que puede absorber señales electrónicas dispersas para que no afecten al dato que está siendo enviado por el núcleo interior del cable. Por esta razón el coaxial es una buena elección para largas distancias y para fiabilidad soportando altos ratios de datos con equipo poco sofisticado.

### 3.3.3 Cable de Par Trenzado

En su forma más simple, el cable de par trenzado consiste en dos filamentos de hilo de cobre girados uno sobre otro. Hay tres tipos de cable de par trenzado: Par Trenzado no blindado (UTP), Par Trenzado blindado (STP) y Par trenzado con blindaje global (FTP).

Un número de pares trenzados es agrupado a menudo junto y encerrado en una funda protectora para formar un cable. El actual número de pares en un cable varía. Los giros cancelan el ruido eléctrico desde los pares adyacentes y desde otras fuentes como motores y transformadores.

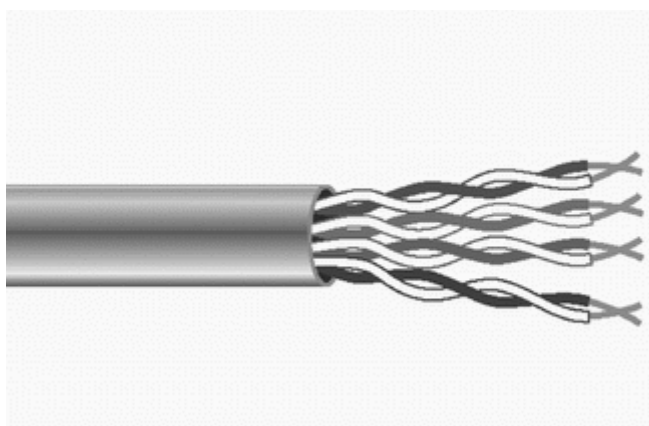


Fig. 11  
Cable Par Trenzado



### 3.3.4 UTP. Par trenzado no blindado (no aislado)

Son cables de pares trenzados sin apantallar que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

UTP está especificado en el estándar EIA/TIA 568. EIA/TIA 568 usó UTP en la creación de estándares que aplicó a una variedad de edificios y situaciones de cableado, asegurando consistencia de productos para los clientes.

Esos estándares incluyen cinco categorías de UTP:

- Categoría 1. Esta se refiere al cable telefónico UTP tradicional que transporta voz pero no datos. La mayoría del cable telefónico anterior a 1983 era de Categoría 1.
- Categoría 2. Esta categoría certifica el cable UTP para transmisión de datos hasta 4 Mbps (megabits por segundo). Consiste en 4 pares trenzados.
- Categoría 3. Esta categoría certifica el cable UTP para transmisiones de datos hasta 10 Mbps. Consiste en 4 pares girados con 3 vueltas por pie.
- Categoría 4. Esta categoría certifica el cable UTP para transmisiones de datos hasta 16 Mbps. Consiste en 4 pares trenzados.
- Categoría 5. Esta categoría certifica el cable UTP para transmisión de datos hasta 100 Mbps. Consiste en 4 pares trenzados de cobre. De los 8 hilos solo se usan 4.

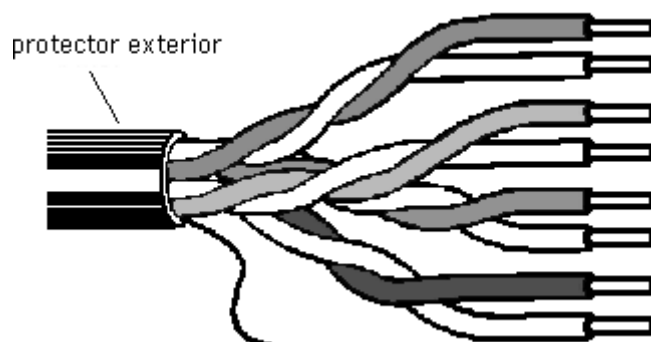


Fig. 12

De hecho, una razón por la que UTP es tan popular es porque muchos edificios están pre-cableados para sistemas telefónicos de par trenzado. Como parte de este pre-cableado, extra UTP es a menudo instalado para cumplir las futuras necesidades. Si el cable pre-instalado es de grado suficiente para soportar transmisión de datos, puede ser usado en una red de ordenadores.

Se requiere precaución, sin embargo, porque el cable telefónico normal puede no tener los giros y otras características eléctricas requeridas para una transmisión de datos limpia y segura.

Un problema potencial con todos los tipos de cables es el crosstalk (Diafonía).

UTP es particularmente susceptible al crosstalk. El aislamiento se usa para reducir crosstalk.

### **3.3.5 STP. Par trenzado aislado.**

STP usa un canutillo o camisa que envuelve la trenza de cobre que es de alta calidad, y más protectora que la del UTP. STP también usa un recubrimiento entre y alrededor de los pares y el giro interno de los mismos. Esto da a STP un excelente aislamiento para proteger los datos transmitidos de interferencias del exterior.

Esto es lo que hace que STP sea menos susceptible a interferencias eléctricas y soporte más altos ratios de transmisión a más largas distancias que UTP.



Fig. 13

Componentes del cable de par trenzado.

- Hardware de conexión. Par trenzado usa conectores telefónicos RJ-45 para conectarse a un ordenador. Es similar al conector telefónico RJ-11. Además se parecen a primera vista, pero hay diferencias cruciales entre ellos. El RJ-45 es ligeramente más largo, y no cabe en el enchufe del RJ-11. El RJ-45 tiene 8 conexiones de cable, mientras que el RJ-11 solo cuatro.
- Están disponibles varios componentes para ayudar a organizar grandes instalaciones UTP y hacer más fácil trabajar con él:
  - Anaqueles de distribución (racks) y los racks en sí mismos.
  - Los racks de distribución y los racks en sí mismos pueden crear más espacio para cables allí donde no hay mucho.
  - Es una buena forma para centralizar y organizar una red que tenga un montón de conexiones.
  - Paneles de expansión (Patch Panels)
  - Hay varias versiones que soportan hasta 96 puntos y velocidades de transmisión de 100 Mbps.
  - Latiguillos o ladrones. Conectores RJ-45 simples o dobles para los patch panels o rosetas de pared y soportan ratios de 100 Mbps.
  - Rosetas de pared. Soportan dos o más pares.

### **3.3.6 FTP. Par trenzado con blindaje global.**

En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas.

Su impedancia característica típica es de 120 OHMIOS y sus propiedades de transmisión son más parecidas a las del UTP. Además puede utilizar los mismos conectores RJ45.



Fig. 14

Tiene un precio intermedio entre el UTP y STP.

### **3.3.7 Cable de Fibra Óptica**

En este cable, las fibras ópticas transportan señales de datos digitales en forma de pulsos modulados de luz. Es una forma relativamente segura de enviar datos ya que no se envían impulsos eléctricos por el cable de fibra óptica.

Esto hace que el cable de fibra óptica no pueda ser derivado y los datos robados, lo que es posible con cualquier cable basado en cobre transportando datos en forma de señales electrónicas.

El cable de fibra óptica es bueno para muy alta velocidad. Tiene alta capacidad de transmisión de datos debido a la ausencia de atenuación y la pureza de la señal.

## Composición de la Fibra Óptica

La fibra óptica consiste en un cilindro de vidrio extremadamente fino, llamado núcleo, envuelto por una capa concéntrica de vidrio conocida como el “vestido”. Las fibras están hechas a veces de plástico.

El plástico es fácil de instalar, pero no puede llevar los pulsos de luz tan lejos como el vidrio.

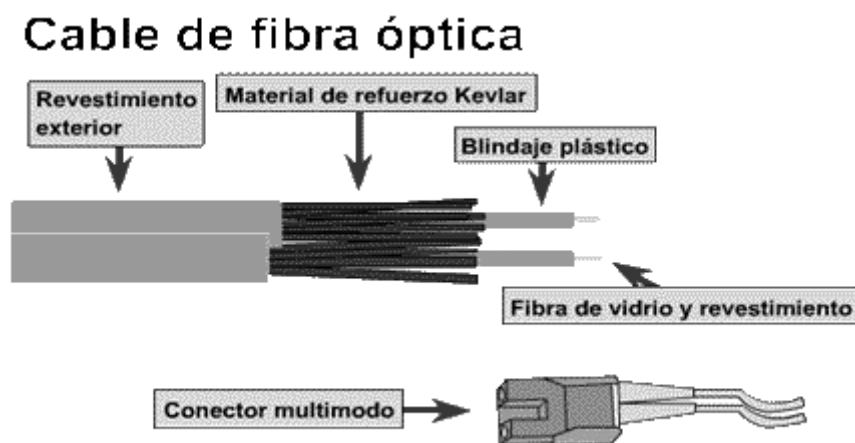


Fig. 15  
Cable de Fibra Óptica

Cada filamento de vidrio pasa señales en una única dirección, por eso el cable consiste en dos filamentos en camisas separadas. Uno transmite y el otro recibe. Una capa de plástico reforzado envuelve cada filamento de vidrio mientras que fibras de Kevlar proporcionan resistencia. Las fibras de Kevlar en el conector de fibra óptica están situadas entre los dos cables, que están encapsulados en plástico.

Las transmisiones en cable de fibra óptica no están sujetas a interferencia eléctrica y son extremadamente rápidas (actualmente alrededor de 100 Mbps con ratios demostrados de hasta 200.000 Mbps)

Puede transportar la señal, el pulso de luz, a millas. La luz puede viajar en monomodo y multimodo, rebotando por las paredes del filamento.

Consideraciones para la Fibra Óptica:

- Deberá usarse cable de fibra óptica, si se necesita transmitir a muy altas velocidades sobre largas distancias en un medio muy seguro.
- No debe usarse cable de fibra óptica, si no se cuenta con un buen presupuesto.

Tipos de cable de fibra óptica.

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

Fibra Multimodo.

Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 km; es simple de diseñar y económico.

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

Fibra Monomodo.

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra.

A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s).

### Seleccionando el cableado

Para determinar qué cableado es el mejor, para un lugar en particular podemos hacernos las siguientes preguntas:

- Cuán pesado será el tráfico en la red.
- Cuáles son las necesidades de seguridad de la red.
- Cuáles son las distancias que debe recorrer el cable.
- Cuáles son las opciones de cable.
- Cuál es el presupuesto de cableado.

La mayoría de los cables protegen contra el ruido eléctrico interno y externo, aunque sea muy lejos y muy rápido, podrán transportar una señal limpia. Sin embargo, cuanto mayor velocidad, claridad y seguridad, más caro será.

## CAPITULO IV

### SOFTWARE PARA LA ADMINISTRACIÓN DE REDES LAN

La Administración de red es la forma de aprovechar al máximo los recursos tanto físicos como internos de la red, manteniéndola operativa y segura para los usuarios. En una administración de red interactúan varios factores que trabajan conjuntamente para proporcionarnos información sobre la situación en que se encuentra nuestra red, y darle posible solución.

#### 4.1 OBJETIVOS DE LA ADMINISTRACIÓN DE REDES LAN.

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.
- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.



- Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA.
- El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, OS/2.
- Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI, 100vg-Any LAN y Fiber channel.
- Varios métodos de compresión, códigos de línea, etc.

El sistema de administración de red opera bajo los siguientes pasos básicos:

- 1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
- 2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
- 3.- Transportación de la información del equipo monitoreado al centro de control.
- 4.- Almacenamiento de los datos coleccionados en el centro de control.
- 5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
- 6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistemas de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes.

#### **4.1.1 Elementos involucrados en la administración de red**

- A) Objetos: son los elementos de más bajo nivel y constituyen los aparatos administrados.
- B) Agentes: un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:
- Notificación de problemas.
  - Datos de diagnóstico.
  - Identificador del nodo.
  - Características del nodo.
- C) Administrador del sistema: Es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

#### **4.1.2 Operaciones de la administración de red**

Las operaciones principales de un sistema de administración de red son las siguientes:

##### **Administración de fallas.**

La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- a) Detección de fallas.
- b) Diagnóstico del problema.
- c) Darle la vuelta al problema y recuperación.
- d) Resolución.
- e) Seguimiento y control.

### **Control de fallas.**

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

### **Administración de cambios.**

La administración de cambios comprende la planeación, la programación de eventos e instalación.

### **Administración del comportamiento.**

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

### **Servicios de contabilidad.**

Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.

### **Control de Inventarios.**

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

## **Seguridad.**

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

- Identificación y autenticación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad. Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración, rendimiento, seguridad e inventarios.

Dentro de las operaciones de seguridad que se realizan en la administración de redes se encuentra lo que se conoce como llave privada que a continuación se define.

### **Llave privada**

En éste método los datos del transmisor se transforman por medio de un algoritmo público de criptografía con una llave binaria numérica privada solo conocida por el transmisor y por el receptor.

El algoritmo más conocido de este tipo es el DES (Data Encryption Standard).

El algoritmo opera así:

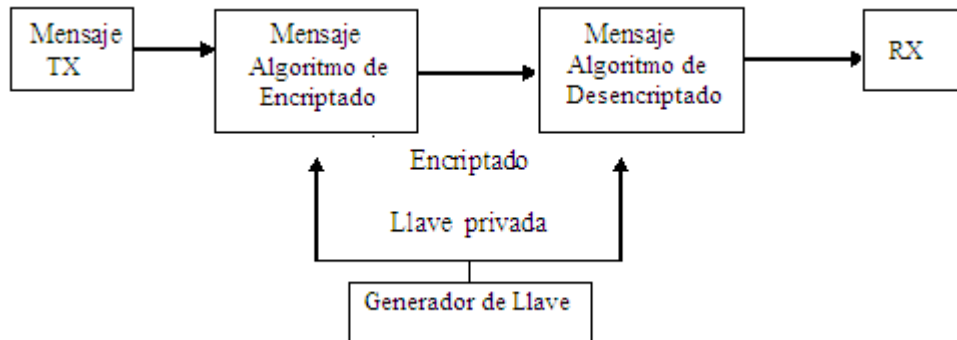


Fig. 16

#### 4.1.3 Funciones de administración definidas por OSI

A principios de 1980 el desarrollo de redes surgió con desorden en muchos sentidos. Se produjo un enorme crecimiento en la cantidad y tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Con base en esto OSI define las cinco funciones de administración básicas siguientes:

- Configuración
- Fallas
- Contabilidad
- Comportamiento
- Seguridad.

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

La función de fallas incluye la detección, el aislamiento y la corrección de fallas en la red.

La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red.

La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.

La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

El modelo OSI incluye cinco componentes claves en la administración de red:

CMIS: Common Management Information Services. Éste es el servicio para la colección y transmisión de información de administración de red a las entidades de red que lo soliciten.

CMIP: Common Management Information Protocol. Es el protocolo de OSI que soporta a CMIS, y proporciona el servicio de petición/respuesta que hace posible el intercambio de información de administración de red entre aplicaciones.

SMIS: Specific Management Information Services. Define los servicios específicos de administración de red que se va a instalar, como configuración, fallas, contabilidad, comportamiento y seguridad.

MIB: Management Information Base. Define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información en el MIB incluye: número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad, etc.

Servicios de Directorio: Define las funciones necesarias para administrar la información nombrada, como la asociación entre nombres lógicos y direcciones físicas.

#### 4.1.4 Administración definida por SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

#### COMPONENTES BÁSICOS.

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados;
- Agentes;
- Sistemas administradores de red (NMS's).

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS deben existir en cualquier red administrada.

Cuando el aparato controlado no soporta SNMP, se usa un agente Proxy. El agente Proxy actúa como un intermediario entre la aplicación de administración de red y el aparato no soporta SNMP.

Administración de un aparato que no soporta SMMP:

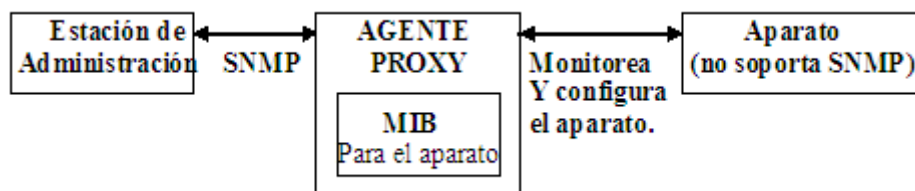


Fig. 17

## MENSAJES SNMP.

El administrador de red de la estación de control y los agentes instalados en los aparatos manejados se comunican enviando mensajes SNMP. Sólo hay 5 mensajes:

Get request: Contiene una lista de variables que el administrador desea leer de una MIB; es decir, el administrador pregunta a un agente sobre el estado de un objeto.

Get Next request: Este comando provee un modo de leer secuencialmente una MIB.

Set request: El administrador usa este comando para ordenar un cambio en el valor de una o más variables.



Get response: El agente envía este mensaje como réplica a un mensaje de Get request, Get next request o Set request.

Trap: El agente usa este mensaje para informar que ha ocurrido un hecho significativo:

- falla de un enlace local.
- otra vez funciona el enlace.
- mensaje recibido con autenticación incorrecta.

Un mensaje SNMP debe estar totalmente contenido en un datagrama IP, el cuál por omisión, es de 576 bytes, por lo que su tamaño puede llegar a ser de hasta 484 bytes.

#### TIPOS DE DATOS DE SNMP.

SNMP maneja los siguientes tipos de datos:

Enteros: Para expresar, por ejemplo, el MTU (Maximum Transfer Unit).

Dirección IP: Se expresa como cuatro bytes. Recuérdese que cada elemento de red se configura con al menos una dirección IP.

Dirección física: Se expresa como una cadena de octetos de longitud adecuada; por ejemplo, para una red Ethernet o Token Ring, la dirección física es de 6 octetos.

Contador: Es un entero no negativo de 32 bits, se usa para medir, por ejemplo, el número de mensajes recibidos.

Tabla: es una secuencia de listas.

Cadena de Octetos: Puede tener un valor de 0 a 255 y se usa para identificar una comunidad.

#### **4.1.5 Base de datos de administración: MIB**

La MIB define los objetos de la red operados por el protocolo de administración de red, y las operaciones que pueden aplicarse a cada objeto. Una variable u objeto MIB se define especificando la sintaxis, el acceso, el estado y la descripción de la misma. La MIB no incluye información de administración para aplicaciones como Telnet, FTP o SMTP, debido que es difícil para las compañías fabricantes instrumentar aplicaciones de este tipo para el MIB.

Sintaxis: Especifica el tipo de datos de la variable, entero, cadena dirección IP, etc.

Acceso: Especifica el nivel de permiso como: Leer, leer y escribir, escribir, no accesible.

Estado: Define si la variable es obligatoria u opcional.

Descripción: Describe textualmente a la variable.

La MIB-1 define solo 126 objetos de administración, divididos en los siguientes grupos:

##### **Grupo de Sistemas.**

Se usa para registrar información del sistema el cual corre la familia de protocolos, por ejemplo:

- Compañía fabricante del sistema.
- Revisión del Software.
- Tiempo que el sistema ha estado operando.

##### **Grupo de Interfaces.**

Registra la información genérica acerca de cada interface de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, MTU del aparato, etc.

### **Grupo de traducción de dirección.**

Comprende las relaciones entre direcciones IP y direcciones específicas de la red que deben soportar, como la tabla ARP, que relaciona direcciones IP con direcciones físicas de la red LAN.

### **Grupo IP.**

Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc.

También contiene información de variables de control que permite aplicaciones remotas puedan ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP.

### **Grupo TCP**

Este grupo incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activas como dirección IP, puerto o estado actual.

### **MIB-II.**

La MIB –II pretende extender los datos de administración de red empleados en redes Ethernet y Wan usando ruteadores a una orientación enfocada a múltiples medios de administración en redes LAN y Wan. Además agrega dos grupos más:

### **Grupo de Transmisión.**

Grupo que soporta múltiples tipos de medios de comunicación, como cable coaxial, cable UTP, cable de fibra óptica y sistemas TI/EI.

## **Grupo SNMP.**

Incluye estadísticas sobre tráfico de red SNMP.

Cabe señalar que un elemento de red, solo necesita soportar los grupos que tienen sentido para él.

### **4.1.6 Seguridad en la administración de redes**

En redes de computadoras, como en otros sistemas, su propósito es de reducir riesgos a un nivel aceptable, con medidas apropiadas. La seguridad comprende los tópicos siguientes:

- a) **Identificación: (ID)** es la habilidad de saber quién es el usuario que solicita hacer uso del servicio.
- b) **Autenticación:** Es la habilidad de probar que alguien es quien dice ser; prueba de identidad. Por ejemplo un password secreto que solo el usuario debe conocer.
- c) **Control de Acceso:** una vez que se sabe y se puede probar que un usuario es quien es, el sistema decide lo que le permite hacer.
- d) **Confidencialidad:** Es la protección de la información para que no pueda ser vista ni entendida por personal no autorizado.
- e) **Integridad:** Es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.

- f) No repudiación: La no repudiación es la prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que el emisor del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido. La propiedad de no repudiación de un sistema de seguridad de redes de cómputo se basa en el uso de firmas digitales.

#### **4.1.7 Software para administrar redes LAN**

Existen diversos programas para poder administrar una red LAN de manera eficiente y segura, a continuación haremos mención de algunos de estos programas y algunas de sus funciones más importantes, además podremos observar algunas imágenes de dichos programas, mencionaremos sólo algunos ya que existe una gran variedad de ellos y los siguientes programas en particular son muy eficientes, ligeros y amigables con el usuario además de que algunos los podemos encontrar en español y gratuitos.

##### **LANHELPER.**

LanHelper es un eficaz administrador de red local (LAN) que nos ayuda a gestionar mejor la red local que controlemos, facilitándonos el control de todos los sistemas conectados a la misma.

Una de las ventajas de esta herramienta es que no necesita instalar ningún tipo de aplicación en el resto de las computadoras, basta con instalarlo en la máquina que usaremos como administrador.

El programa realiza un rápido análisis de la red y muestra en su interfaz una lista de todas las máquinas que forman parte de ella, con numerosos datos informativos sobre cada una de ellas: nombre de la PC, dirección IP, dirección MAC, sistema operativo, etc.

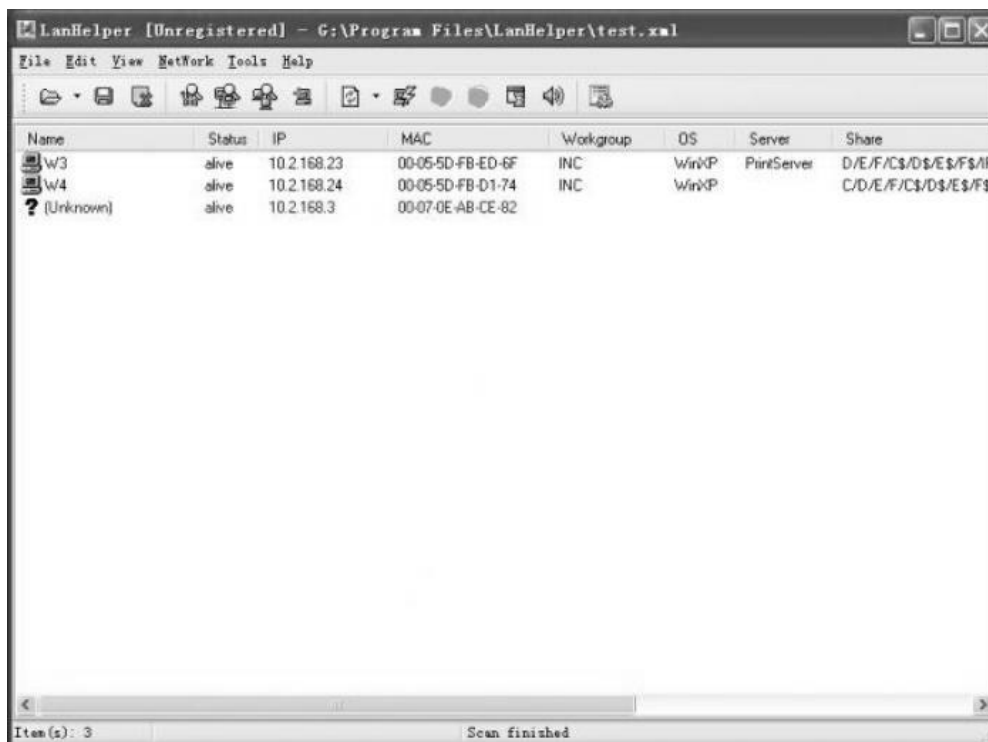


Fig. 18

Desde la propia interfaz también podemos enviar mensajes, apagar o reiniciar remotamente los ordenadores, detectar el estado del sistema e incluso ejecutar procesos en las máquinas remotas.

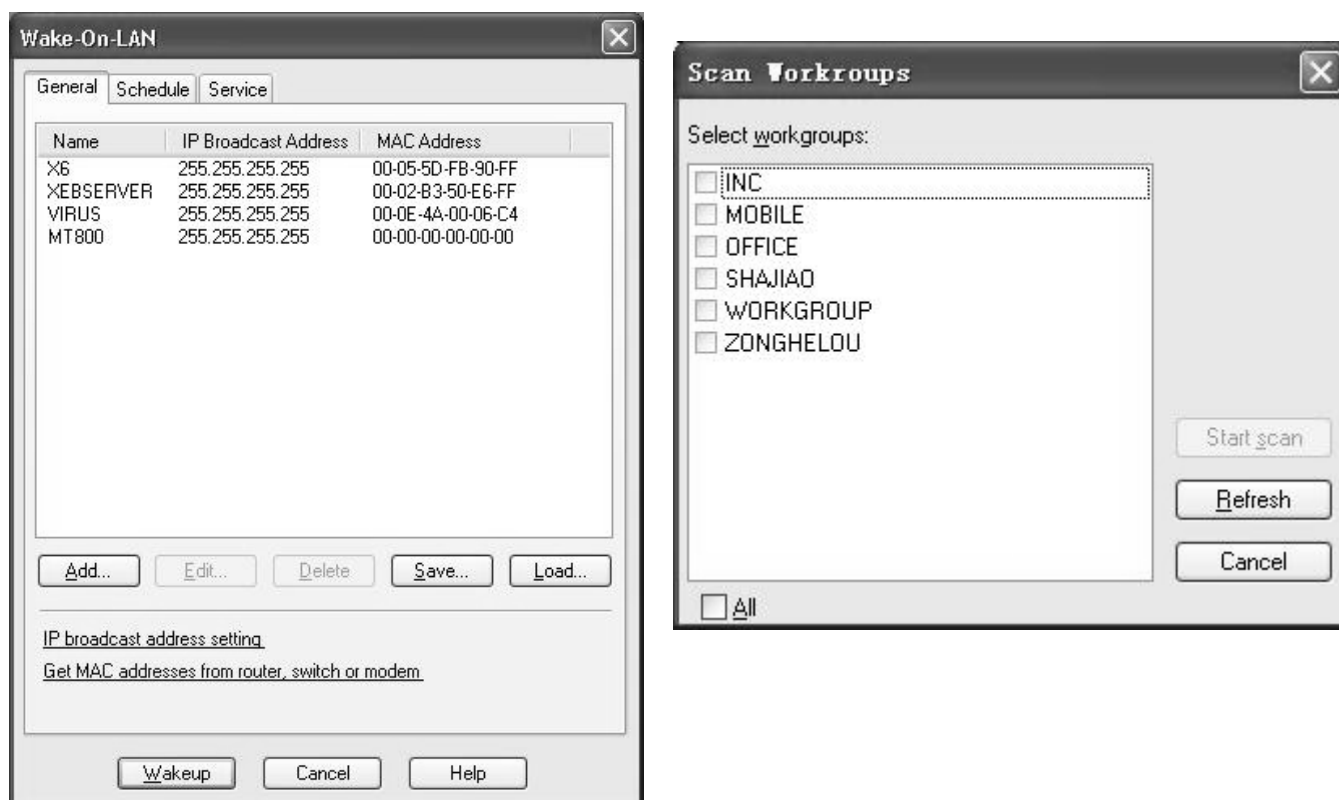


Fig. 19

Cabe mencionar que este programa a partir de la versión 1.92 lo podemos encontrar en idioma español. A diferencia de otros programas LanHelper no necesita ser instalado en todas las computadoras que forman la red, esta es una cualidad que hace de éste un programa interesante y fácil de utilizar.

## LANTOOL.

El programa incluye las funciones propias de cualquier aplicación del estilo como suele ser apagar, reiniciar o encender ordenadores de forma remota.

En la pantalla principal aparecerán todos los equipos sobre los que tenemos control. Haciendo click con el botón derecho en cada uno de ellos podremos realizar bastantes opciones diferenciadas en 5 categorías básicas: operaciones de sistema, mensajería, estado de la Red, miscelánea e info.

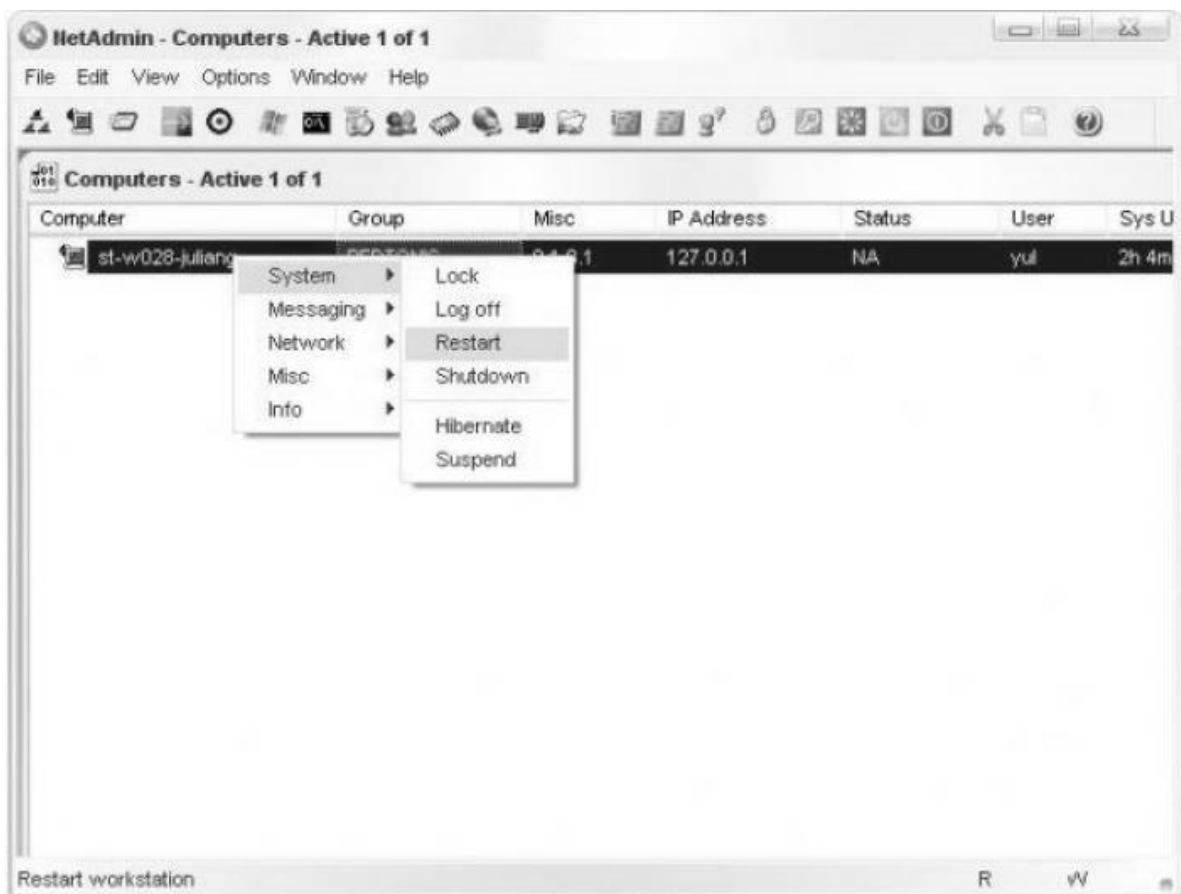


Fig. 20



También es capaz de enviar archivos a PC, determinar si existen problemas de velocidad entre dos puntos de la red, realizar pruebas de calidad de la red, finalizar procesos remotamente, etc.

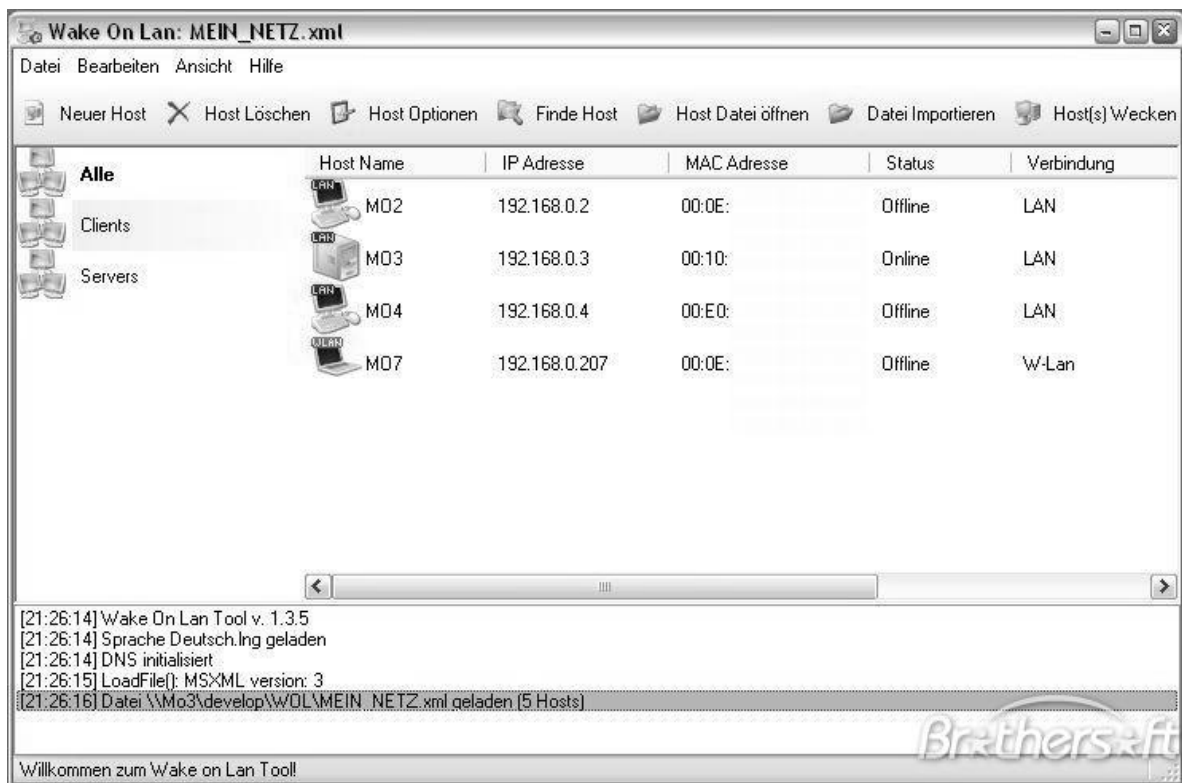


Fig. 21

Incluye una curiosa función para bajarle el volumen a alguien que pueda estar reproduciendo música demasiado alto y pueda estar molestando a otras personas.

Una de las grandes ventajas de este programa es que podemos encontrarlo de manera gratuita y no es muy pesado a diferencia de otros, además no ocupa mucha memoria en nuestro equipo, quizás el único inconveniente es que esta en el idioma ingles.

## NETWORK MANAGEMENT.

Otro programa muy útil es Network Management, una utilidad para instalar, configurar o desinstalar aplicaciones de forma remota en ordenadores conectados en una red local.

Una gran utilidad de este programa es que podemos programar que se instale un determinado programa (una actualización de un antivirus por ejemplo), se ejecute, compruebe que no hay virus y tome una captura. Lo mejor es que podemos hacer cualquier cosa simultáneamente en todas las PC de la red y programarla para que se ejecute periódicamente.

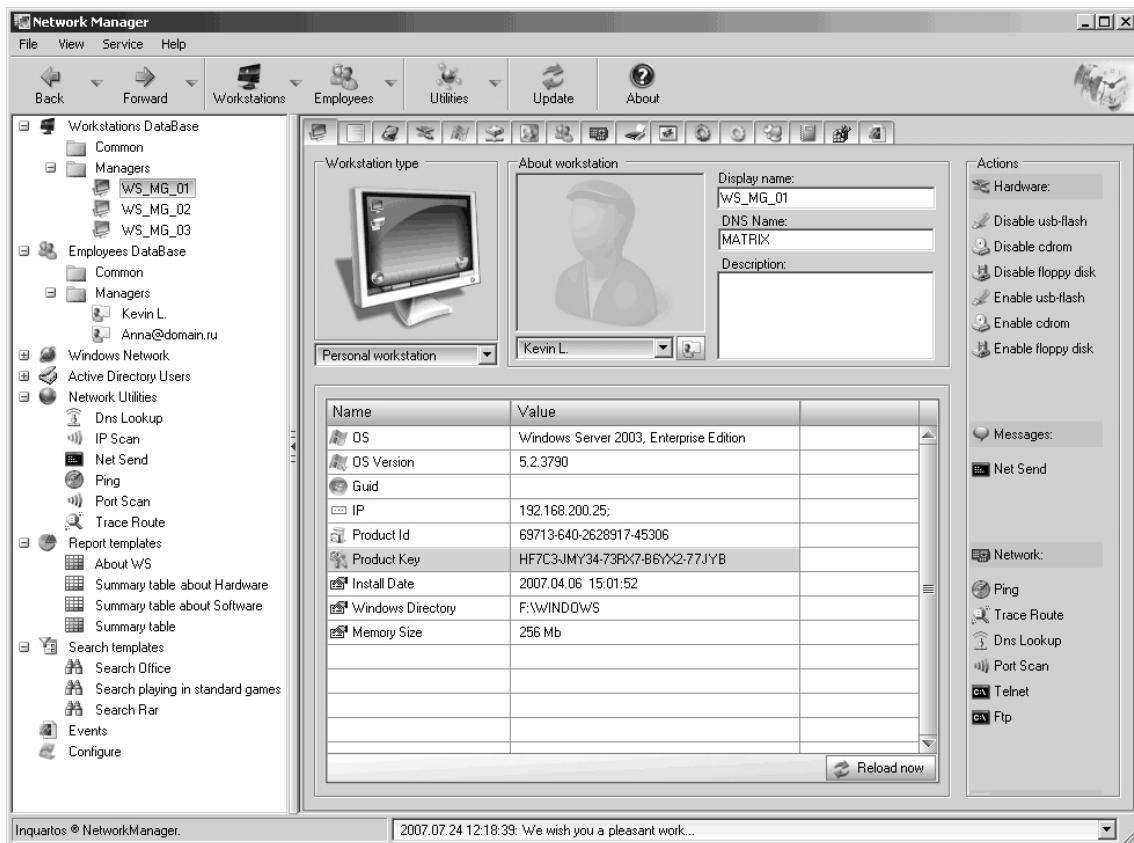


Fig. 22

Una de sus funciones más interesantes es que podemos cargar el administrador de procesos del PC remoto, pudiendo ver lo que se está ejecutando, matar procesos, ver la carga del CPU y memoria, etc.

Este programa podemos encontrarlo en el idioma inglés y es totalmente gratuito en su versión 1.43

## **ETHER PEEK**

Ether peek es uno de los productos más importantes de la empresa Wildpackets, el cual se encarga de realizar el análisis, monitoreo y seguimiento de los protocolos de una LAN sobre tecnología Ethernet, ofrece diagnósticos y acción en tiempo real. También realiza gestiones para la detección de posibles errores mediante un análisis detallado de lo que sucede.

Etherpeek funciona en cualquier máquina que soporte el sistema operativo especificado, en este caso la mayoría funciona sobre plataforma Windows, con una máquina que tenga buena capacidad de procesamiento (256 MB en RAM) y con una tarjeta de red ya sea Ethernet o PCMCIA (tarjeta de red externa).

El funcionamiento principal de Etherpeek se basa en tres consideraciones, las cuales obtienen las principales funciones de Etherpeek de manera general:

- Análisis de paquetes que se circulan en la red.
- Obtener mediante archivos en distintos formatos, el diagnóstico y análisis de los paquetes y protocolos.
- Detección de posibles fallas y errores en los paquetes y en los protocolos pertenecientes a la red.

El software trabaja en tiempo real lo cual la hace una herramienta bastante rentable.

En general, Etherpeek tiene distintas funciones las cuales ayudan al administrador a realizar toma de decisiones, es decir, las acciones a tomar en base a los diagnósticos y análisis de lo que está sucediendo en la red.

Se debe tomar en cuenta que la versión de Etherpeek para Windows 2000 tiene funciones más limitadas, que versiones más recientes como la de Windows XP, a la cual se le han realizado mejoras en funciones como lo son: estadísticas por gráficos y actualizaciones constantes sobre el surgimiento de nuevos protocolos y ataques en Internet.

Para conocer lo que está pasando realmente en una red LAN, el usuario o administrador debe tener pleno conocimiento de los términos que se manejan en el área de redes, al momento de presentarle algún reporte o un conjunto de datos.

Por lo tanto a continuación se muestran los datos que el administrador podrá observar al momento de realizar el análisis pertinente.

A continuación se muestra una imagen de la interfaz de Etherpeek la cual realiza la tarea de análisis y monitoreo de una LAN.

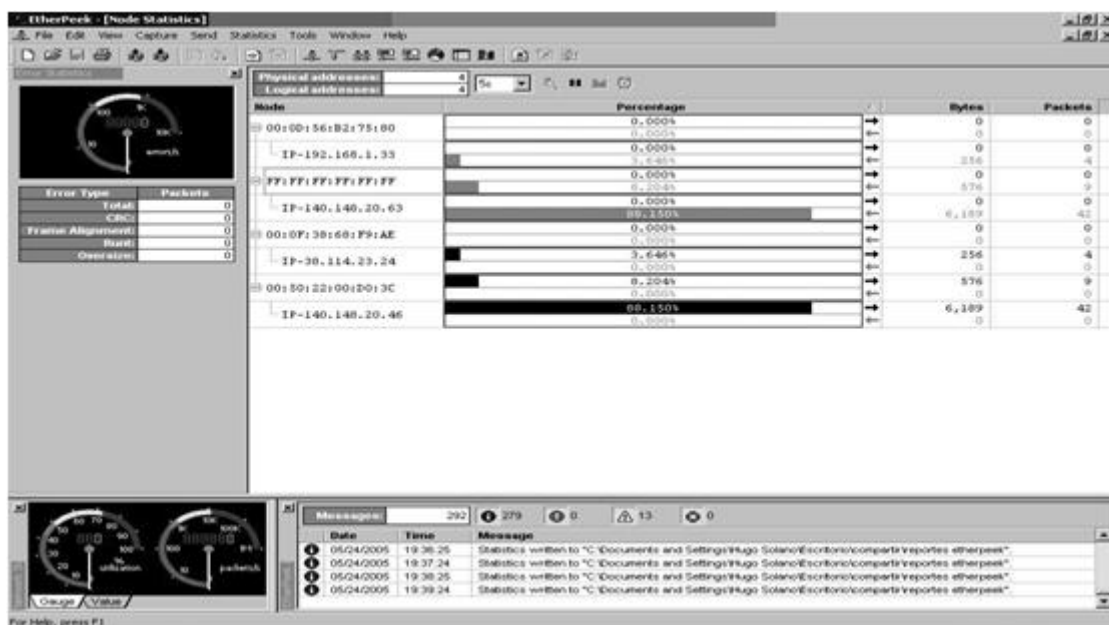


Fig. 23

Reportes sobre el análisis y diagnóstico de la LAN.

Esta función en específico que realiza Etherpeek, es muy importante ya que obtenemos información sobre las características más importantes de nuestra LAN (paquetes de datos enviados y recibidos, protocolos usados, tipos de banderas utilizados por los paquetes, errores de envío y recepción de paquetes), en un formato en donde el usuario pueda visualizarlo de manera desglosada y uniforme.

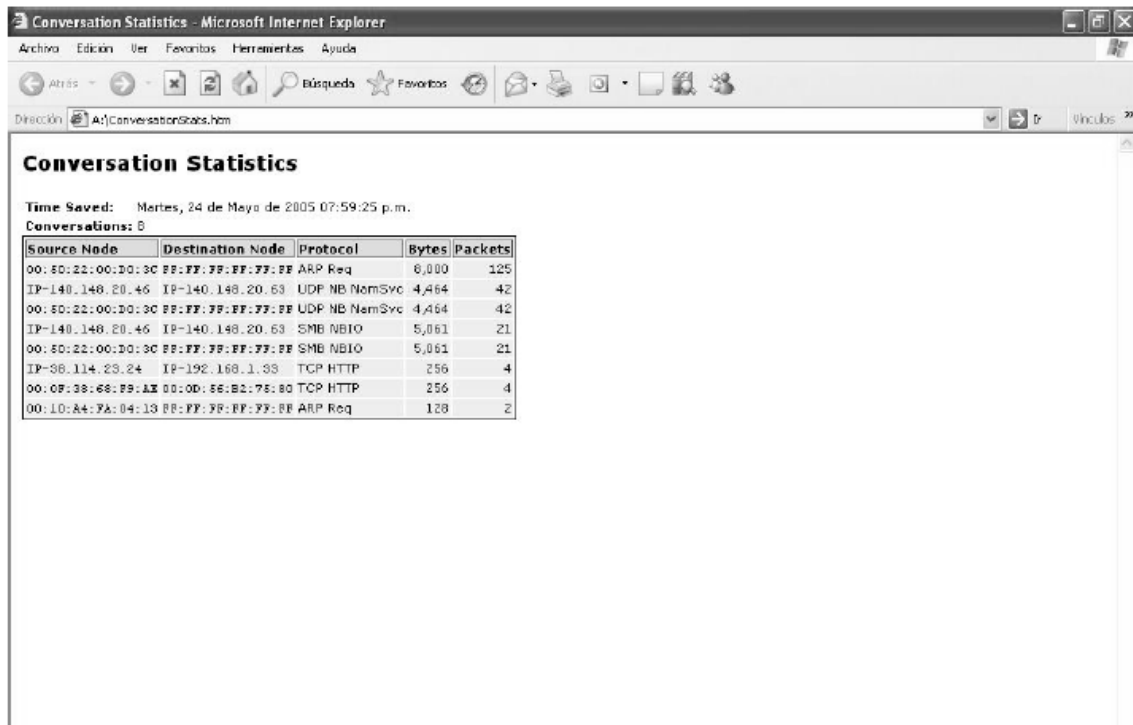
La diferencia entre visualizar este tipo de datos en el software mismo y en base a archivos, es que el usuario tiene la ventaja de crear una carpeta para almacenar los archivos y que se encuentra ordenado por tipo de archivo, en cambio en el software se debe tener un conocimiento acerca de su utilización y estar familiarizado.

Estos archivos que genera Etherpeek son conocidos como reportes, los cuales son documentos detallados para el análisis de la red. Etherpeek puede ser programado o no para lanzar y guardar estos reportes hacia una carpeta en la máquina de manera local.

Los tipos de reportes que guardamos mediante Etherpeek son los siguientes:

- ConversationStats.

Este reporte despliega de manera detallada la actividad de cada uno de los nodos que se encuentran en la red con los siguientes atributos: dirección origen del envío de paquete, dirección destino hacia donde se dirige el paquete, el protocolo utilizado para el envío de paquetes, bytes enviados y paquetes enviados en total.



Conversation Statistics

Time Saved: Martes, 24 de Mayo de 2005 07:59:25 p.m.  
Conversations: 0

Source Node	Destination Node	Protocol	Bytes	Packets
00:50:22:00:20:3C FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ARP Req	6,000	125
IP-140.148.20.46	IP-140.148.20.63	UDP NB NomSvc	4,464	42
00:50:22:00:20:3C FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP NB NamSvc	4,464	42
IP-140.148.20.46	IP-140.148.20.63	SMB NBIO	5,061	21
00:50:22:00:20:3C FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	SMB NBIO	5,061	21
IP-88.114.23.24	IP-192.168.1.33	TCP HTTP	256	4
00:0F:38:68:F9:AX	00:0D:56:B2:76:80	TCP HTTP	256	4
00:1D:A4:FA:04:13	FF:FF:FF:FF:FF:FF	ARP Req	128	2

Fig. 24

NodeStats.

Este reporte despliega la actividad de cada uno de los nodos (dirección lógica y física) y porcentaje de envío o recepción de paquetes en el uso de la red en total, además de campos y bytes y paquetes enviados por cada uno de los nodos.

A continuación se muestra un ejemplo de este tipo de reportes:

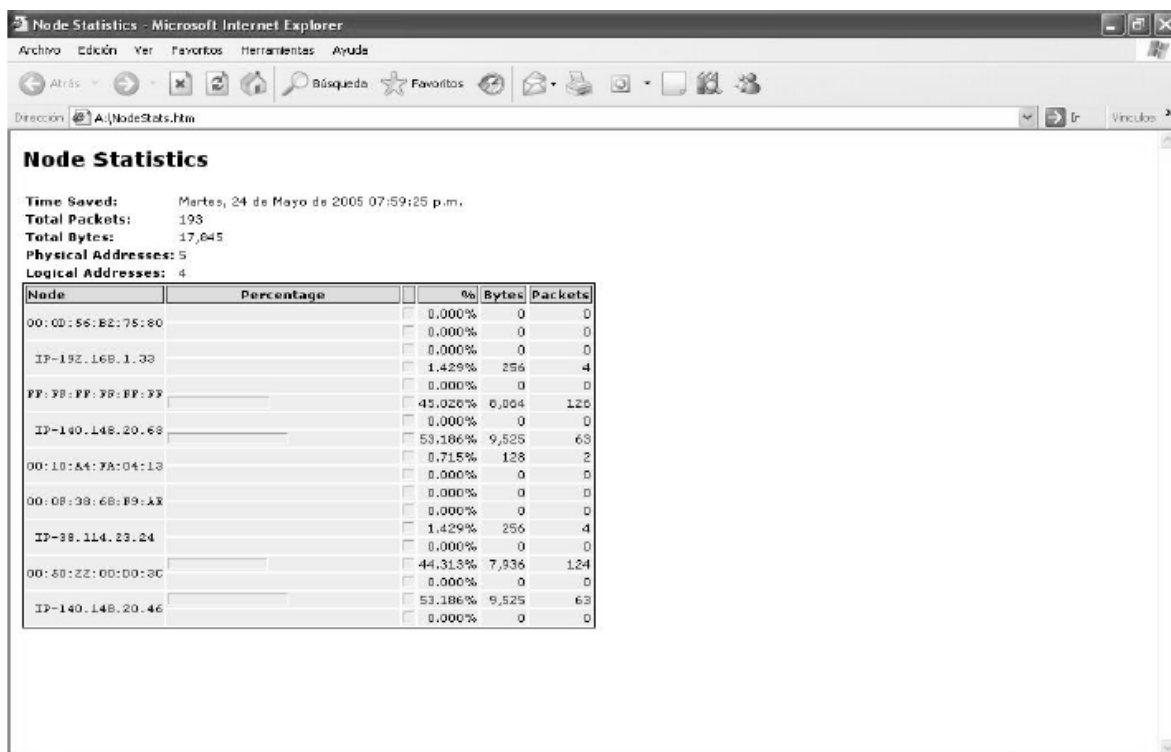


Fig. 25

## Protocol Stats.

Este archivo muestra el porcentaje que existe de cada uno de los protocolos existentes en la red y así saber cuál es el que más predomina.

A continuación se muestra un ejemplo de este tipo de reportes:

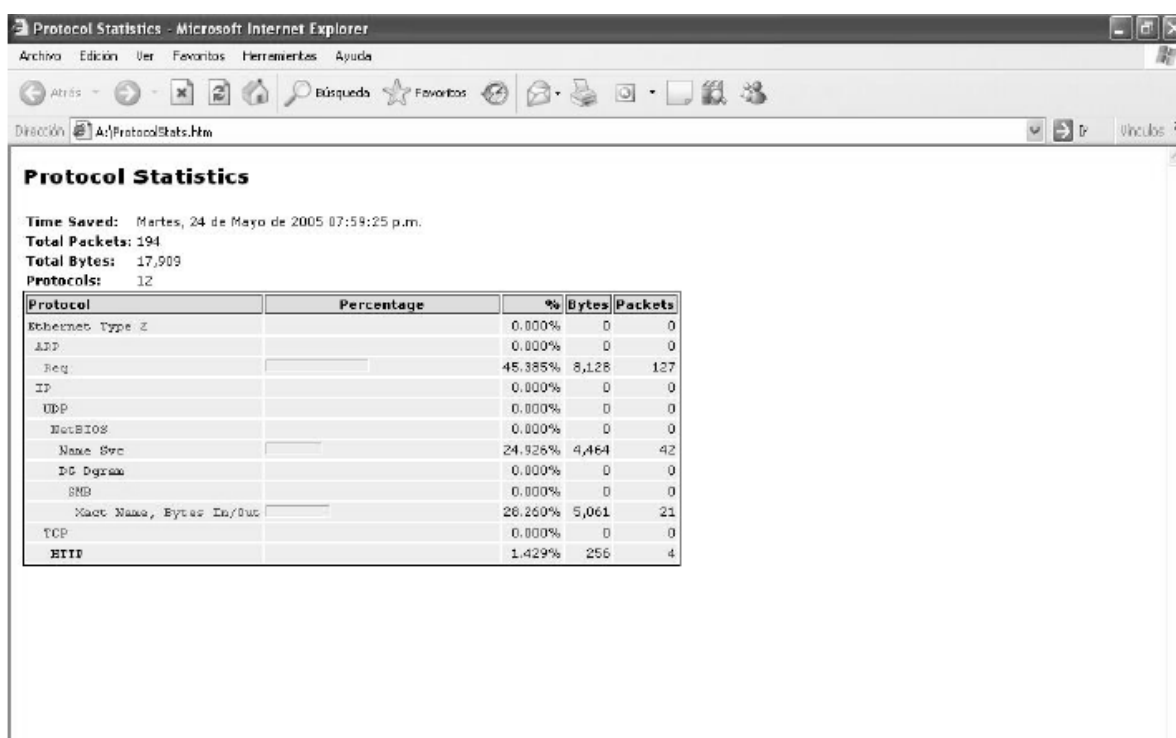


Fig. 26



## Summary Stats

Este tipo de reporte despliega a detalle toda la actividad que pasa en nuestra LAN. Entre otros datos que sobresalen son todos los tipos de paquetes que han pasado en la red, y el tipo de error si llegara a existir por cada uno de los campos que conforman el paquete.

A continuación se muestra un ejemplo de este tipo de reportes:

**Summary Statistics**

Time Saved: Martes, 24 de Mayo de 2005 07:59:25 p.m.  
 Start Time: 05/24/2005 19:30:25  
 Duration: 00:28:59

Group	Stat	Bytes	Packets	B/sec	P/sec	% of B	% of P
General	Start Data	05/24/2005	05/24/2005	05/24/2005	05/24/2005	05/24/2005	05/24/2005
General	Start Time	19:30:25	19:30:25	19:30:25	19:30:25	19:30:25	19:30:25
General	Duration	00:28:59	00:28:59	00:28:59	00:28:59	00:28:59	00:28:59
General	Total Bytes	17,845	-	10.260	-	1.000%	-
General	Total Packets	-	193	-	0.111	-	1.000%
General	Total Broadcast	17,589	189	10.113	0.109	0.986%	0.979%
General	Total Multicast	17,589	189	10.113	0.109	0.986%	0.979%
General	Average Utilization (Kbits/s)	0.089	0.089	0.089	0.089	0.089	0.089
Errors	Total	-	0	-	0.000	-	0.000%
Errors	CRC	-	0	-	0.000	-	0.000%
Errors	Frame Alignment	-	0	-	0.000	-	0.000%
Errors	Runt	-	0	-	0.000	-	0.000%
Errors	Oversize	-	0	-	0.000	-	0.000%
Counts	Physical Addresses Seen	5	5	5	5	5	5
Counts	AppleTalk Addresses Seen	0	0	0	0	0	0
Counts	IP Addresses Seen	4	4	4	4	4	4
Counts	DECnet Addresses Seen	0	0	0	0	0	0
Counts	Protocols Seen	12	12	12	12	12	12
Size Distribution	<= 64	-	190	-	0.075	-	0.674%
Size Distribution	65-127	-	42	-	0.024	-	0.218%
Size Distribution	128-255	-	16	-	0.009	-	0.083%
Size Distribution	256-511	-	5	-	0.003	-	0.026%
Size Distribution	512-1023	-	0	-	0.000	-	0.000%
Size Distribution	1024-1517	-	0	-	0.000	-	0.000%
Size Distribution	>= 1518	-	0	-	0.000	-	0.000%

Fig. 27

## **Protocolos de los paquetes.**

En este campo se muestra el tipo de protocolos de cada uno de los paquetes.

Esto permite que dos computadoras que tengan un sistema operativo o protocolo de comunicación distinto puedan transmitir datos entre ellos.

### **TCP/IP.**

Se considera el protocolo más importante en Internet en donde se juntan los protocolos Transfer Control Protocol (TCP) e Internet Protocol (IP), la función principal de este protocolo es un procedimiento de comunicación general que garantiza la transmisión de datos entre los equipos.

El error más común que se puede encontrar en este protocolo, es realizar la comunicación en el envío de paquetes y recibir una negativa de que no pudo completarse la transferencia de datos al equipo emisor, para que nuevamente se realice la comunicación; en caso de que no exista ninguna comunicación, debe revisarse el equipo el cual cuenta con este protocolo para saber si se encuentra bien configurado.

### **UDP**

Las siglas UDP quieren decir User Datagram Protocol y se considera como un protocolo NO orientado a la conexión y en lugar de entregar paquetes entrega datagramas, en donde la diferencia entre estos dos es que en el paquete hay un control de flujo de errores y en el datagrama no.

Aunque en el datagrama sí se llegan a utilizar funciones de detección de errores, por lo tanto no proporciona ningún tipo de control de errores ni de flujo, aunque sí que utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama en lugar de entregarlo a la aplicación se descarta y no se toma en cuenta.

Las características principales de este protocolo es que no garantiza la fiabilidad al momento de entregar información y entrega la información desordenada y sin ninguna secuencia y por lo tanto es un protocolo más propenso a errores al momento de la transferencia de datos, ya que no se tiene ninguna respuesta de si se recibió la información correctamente.

### Protocolo ARP

El protocolo ARP se denomina como Address Resolution Protocol y se encarga de utilizar un mecanismo de resolución dinámico el cual crea una tabla de equivalencias entre las direcciones MAC (Media Access Control) o sea la dirección física de la computadora y las direcciones IP (Internet Protocol) que son las direcciones lógicas de la computadora.

El ejemplo más común a este protocolo es cuando una máquina necesita la dirección MAC de otra máquina a partir de una dirección IP, entonces la máquina manda lo que se llama un Broadcast ARP Request, que consiste en mandar la dirección IP a todos los equipos con los que se puede comunicar y la computadora que tenga esa dirección IP responderá con ARP Reply el cual contiene su dirección MAC.

El error más común en este protocolo es que exista duplicidad de direcciones IP, no puede existir duplicidad en direcciones MAC ya que es única, pero en las direcciones IP, puede existir la posibilidad que dos máquinas compartan la misma dirección IP y por lo tanto existir un error en la comunicación, con otros equipos en la red.

Esto propicia que los equipos pueden mandar información a cualquiera de las dos direcciones lo cual en su momento, puede interpretarse como inconsistencia y pérdida en el envío y recepción de datos.

## Protocolo HTTP.

El protocolo de transferencia de hipertexto (Hypertext Transfer Protocol) en donde el hipertexto es toda la información y contenido que se maneja en las páginas Web y es el más usado. El funcionamiento de este protocolo consiste en que se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla, es decir, se basa en sencillas operaciones de solicitud/respuesta.

Se basa en el modelo cliente-servidor y que articula los intercambios de información que existen entre los clientes Web y los servidores HTTP. Cabe mencionar además, que este protocolo se encuentra soportado sobre los servicios de conexión del protocolo TCP/IP.

## Protocolo DNS

DNS aunque no es un protocolo en sí, tiene su propia especificación en un paquete de datos, DNS que quiere decir Domain Name Server está basado en la estructura cliente-servidor el cual basa su mayor actividad en el servidor o bien llamado revolvedor, la función principal del servidor es proporcionar la información sobre la relación dirección IP-dominio, este protocolo se basa principalmente en un sistema jerárquico de dominios y sub-dominios.

Esto quiere decir que una vez que se haya configurado el servidor para usar los servidores DNS raíz se puede utilizar recursivamente con otros servidores del mismo tipo y así llegar a conocer cualquier dominio asociado a cualquier dirección IP.

Este protocolo es muy útil ya que el usuario no memoriza las páginas mediante una dirección IP sino mediante un dominio que está conformado por un nombre único en la red.

Protocolo IGMP.

El protocolo IGMP (Internet Group Management Protocol), es usado para la suscripción o anulación de suscripción de/desde grupos de multidifusión. Este protocolo solo se puede llegar a utilizar en redes que requieran de tecnologías de multidifusión (transmisión de archivos de video y audio).

Protocolo 802.1 Spanning Tree

El Spanning Tree Protocol (STP) está definido por la IEEE en su estándar 802.1D y el cual es un protocolo de enlace administrador que proporciona consistencia a la red evitando que existan ciclos indeseables en la red.

Es una tecnología que permite que los equipos que comunican a los equipos en la red (switches, puentes y routers) descubrir ciclos físicos a través de la red.

Nodos de la red monitoreada.

Otra de las características que se presentan en los reportes generados por Etherpeek son los nodos, se le puede considerar un nodo a cada computadora perteneciente a la misma subred y con las cuales se puede tener comunicación y transferencia de información o datos.

Los detalles que se muestran de en cada uno de los nodos son los siguientes.

- Total de bytes.

Aquí se muestra el total de bytes que se detectaron en el tiempo que se hizo el rastreo, se dividen en dos partes: bytes enviados y bytes recibidos.

- Total de paquetes.

Aquí se muestra el total de paquetes que se detectaron en el tiempo en el que se hizo el rastreo de la comunicación entre nuestros equipos y se divide en dos partes: paquetes enviados y paquetes recibidos.

- Paquetes broadcast/multicast.

Los paquetes broadcast son aquellos que son mandados de un equipo a todos los demás pertenecientes a la misma red, los paquetes multicast son similares con la diferencia que los paquetes pueden ser enviados por diferentes emisores a todos los equipos involucrados.

- Bytes broadcast/multicast.

Los bytes broadcast son aquellos que son enviados de un usuario a todos los demás que se encuentran en la misma red, por lo tanto los bytes de tipo multicast son los bytes que son enviados por parte de múltiples usuarios a múltiples destinatarios.

Como se pudo observar en este capítulo se explicaron los principales objetivos de la administración de redes LAN así como los elementos involucrados para llevar a cabo dicha administración.

También pudimos ver que existen en el mercado una gran variedad de utilidades para administrar redes LAN, aquí se explicaron algunos de estos programas tomando en cuenta principalmente su compatibilidad, funcionalidad y su costo.

## CONCLUSIONES

Como hemos visto a lo largo de este trabajo, se han explicado los fundamentos, las características, funciones y otros aspectos de las redes LAN, esperando que sean de utilidad para todas aquellas personas interesadas en el tema de redes de computadoras, de esta manera intento brindar con este trabajo una guía a tener en cuenta en el tema de redes LAN.

Debe destacarse que uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas informáticos.

Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio.

La LAN más difundida, Ethernet, utiliza un mecanismo conocido como CSMA/CD. Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más tarde. Ethernet transfiere datos a 10 Mbits/s, lo suficientemente rápido para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Hay topologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas.

Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios y el control de los recursos de la red.

Espero que al leer este trabajo sirva de provecho y llene las expectativas de todas las personas que decidieron tomar esta tesis como un material de apoyo para sus actividades académicas.



## BIBLIOGRAFÍA

- Tecnologías de Interconectividad de Redes  
Merilee Ford, H. Kim Lew  
  
Prentice Hall, CISCO Systems
  
- Redes de Computadoras  
Andrew S. Tanenbaum  
  
Prentice All, 3ª edición
  
- Revista RED “La revista de redes de computadoras”  
Año VII Febrero 1997 Número 77  
  
Editorial Red S.A. de C.V.
  
- Redes de computadoras, protocolos, normas e interfaces.  
Uyless Black  
  
Macrobit
  
- Tesis de la UNAM “Diseño de una red para el sistema bibliotecario de la UNAM”  
María del Socorro Olmos Viruel
  
- Newtons’s Telecom. Dictionary  
Harry Newton  
  
Flatiron Publishing Inc.

- Manual Network Essential's  
Microsoft Co. 1997
- Fundamentos de Redes Plus, Microsoft Corporation, Mc Graw Hill.

## **GLOSARIO**

### **ADAPTADOR DE RED**

Un adaptador de red permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras.

### **ARCNET**

Es un sistema de red banda base, con paso de testigo (token) que ofrece topologías flexibles en estrella y bus a un precio bajo. Las velocidades de transmisión son de 2.5 Mbits/seg.

### **ANCHO DE BANDA**

Es cuanta información se puede enviar a través de una conexión. Usualmente se mide en bits por segundo. Una página completa de texto en español tiene aproximadamente un tamaño de 16,000 bits. Un modem rápido puede mover como 15,000 bits por segundo. Una pantalla de video en total movimiento requerirá unos 10,000,000 bits por segundo, dependiendo de la compresión.

### **BIT**

(Binary DigiT – Dígito binario) Es un número de un solo dígito en base 2. En otras palabras es 1 ó 0. Es la unidad más pequeña de información computarizada. El ancho de banda generalmente se mide en bits por segundo.

## **BNC**

Conector propio de redes construidas con cable coaxial.

## **BPS**

(Bits por segundo) Es una medida de cuán rápido se mueve la información de un lugar a otro. Un modem de 28.8 puede mover datos a 28,800 bits por segundo.

## **BROADCAST**

Transmisión de un paquete que será recibido por todos los dispositivos en una red.

## **BYTE**

Es un conjunto bits que representan un solo carácter. Usualmente existen 8 bits en un byte, algunas veces más, dependiendo como se está midiendo.

## **CLIENTE**

Es un programa de software que se usa para contactar y obtener información del software del servidor, usualmente a larga distancia. Cada programa “cliente” está diseñado para trabajar con uno o varios tipos de programas del servidor. Así como que cada servidor requiere un tipo específico de cliente. Un buscador de web es un cliente.

## **DIAFONIA**

Es la interacción o acoplamiento entre señales cercanas. Suele ocurrir cuando se acoplan los cables de pares y rara vez en cables coaxiales.

## **DNS**

(Domains Name System) Es un sistema de manejo y administración de nombres de dominio.

## **ETHERNET**

Es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD.

## **FTP**

(File Transfer Protocol – Protocolo de Transferencia de Archivos) Un método muy común para desplazar archivos entre dos sitios Internet. El FTP es una manera especial de acceder (login) a otro sitio Internet con el propósito de enviar o recibir archivos.

Existen numerosos sitios Internet que han establecido accesos públicos a archivos de dominio público obtenido usando FTP accedendo mediante el uso de la cuenta anónima por eso se les llama servidores FTP anónimos.

## **GATEWAY**

El significado es el referido a un hardware o software configurado de tal manera, que traduce o transcribe entre dos protocolos diferentes. Por ejemplo, Prodigy tiene un portal que traduce entre su correo electrónico propio e interno y el formato de e-mail del Internet. Otro significado, aunque no muy académico, es el de definirse como un mecanismo que le permite y provee acceso a otro sistema. Por ejemplo, AOL (America on-line) se autoproclama como “portal al Internet”.

## **HOST**

Es cualquier computadora o network que es depositaria de servicios disponibles a otras computadoras en la red. Es común tener una computadora host que provee varios servicios como WWW y USENET.

## **HTTP**

(HyperText Transport Protocol) Es el protocolo para mover archivos de hipertexto a través del Internet. Para su uso, se requiere un programa cliente HTTP en un lado, y un programa servidor HTTP en el otro lado. Actualmente en la www, el HTTP es el protocolo que más se usa en la www.

## **HUB**

Un concentrador o hub es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

## **IP NUMBER**

(Internet Protocol Number) Llamado muchas veces una cuadrícula punteada. Es un número único que consiste de 4 partes separada por puntos. Por ejemplo: 165.113.245.2

Cada computadora que está en la Internet tiene un número IP. Si no tuviese un número Ip, no estaría realmente en el Internet. Muchas computadoras tienen uno o más Nombres de Dominio, los cuales son más fáciles de recordar.

## **LAN**

(Local Area Network – Red Local) Es una red de computadoras que generalmente se encuentran dentro de un edificio o un piso.

## **MODEM**

(MOdulator, DEModulator) Es un aparato conectado a su computador y a una línea telefónica, que permite a un computador “conversar” con otro computador a través de la red telefónica. Básicamente los modem hacen para las computadoras, lo que los teléfonos hacen para las personas.

## **NETWORK**

Cada vez que 2 computadoras se conectan entre sí, se convierten en una red (network).  
Cada vez que 3 redes se conectan entre sí, tenemos Internet.

## **RJ-11**

Conector de 6 pines usado para conexiones de líneas telefónicas que puede utilizar 4 o 6 hilos.

## **RJ-45**

Conector de 8 pines utilizado en las transmisiones de datos por líneas serie.

## **ROUTER O RUTEADOR**

Es una computadora de propósito definido (o paquete de software) que maneja las conexiones entre dos o más redes. Los ruteadores se pasan el tiempo buscando las direcciones de destino para enviar por la mejor ruta los paquetes de información pasando a través de ellos.

## **SERVER O SERVIDOR**

Es una computadora o un paquete de programas (software) que provee una clase específica de servicio a un software “cliente” ubicado en otra computadora. El término se puede referir a una determinada clase de software como el servidor www, o a la computadora donde corre el mencionado software. Por ejemplo, nuestro servidor de correos está caído hoy, por lo que hoy no tendremos correo ni de entrada ni salida. Una sola computadora puede alojar varios paquetes de software de servidor corriendo en ella, y así proveer de varios servicios a clientes de la red.

## **TCP/IP**

(Transmission Control Protocol / Internet Protocol) Protocolo de Control de Transmisión / Protocol de Internet. Es la suite de los protocolos que define el Internet. Se diseñó originalmente para los sistemas operativo UNIX. El software de TCP/IP está disponible para cualquier sistema operativo actualmente. Para estar en la Internet es necesario que su computadora tenga software TCP/IP para que sea eficiente.

## **WAN**

(Wide Area Network) Red de área amplia. Es una red que cubre más extensión que la de un edificio o complejo de edificios.

## **WWW (Web)**

(World Wide Web) Tiene 2 significados: Primero, y el más usado, es el conjunto o constelación de recursos que se pueden acceder usando Gopher, FTP, telnet, USENET, WAIS y algunas otras herramientas. La segunda, el universo de servidores de hipertexto (HTTP) que permiten texto, gráficos, archivos de sonido, etc., y que se pueden mezclar.