

REPOSITORIO ACADÉMICO DIGITAL INSTITUCIONAL

Administración y Configuración de redes locales Microsoft

Autor: Marco Antonio Barrera Argüello

**Tesis presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic.]**

**Nombre del asesor:
Sergio Francisco Barraza Ibarra**

Este documento está disponible para su consulta en el Repositorio Académico Digital Institucional de la Universidad Vasco de Quiroga, cuyo objetivo es integrar organizar, almacenar, preservar y difundir en formato digital la producción intelectual resultante de la actividad académica, científica e investigadora de los diferentes campus de la universidad, para beneficio de la comunidad universitaria.

Esta iniciativa está a cargo del Centro de Información y Documentación "Dr. Silvio Zavala" que lleva adelante las tareas de gestión y coordinación para la concreción de los objetivos planteados.

Esta Tesis se publica bajo licencia Creative Commons de tipo "Reconocimiento-NoComercial-SinObraDerivada", se permite su consulta siempre y cuando se mantenga el reconocimiento de sus autores, no se haga uso comercial de las obras derivadas.





**UNIVERSIDAD
VASCO DE QUIROGA**

Licenciatura en Sistemas Computarizados

**"Administración y Configuración
de Redes Locales Microsoft"**

T E S I S

Que para Obtener el Título de:
Licenciado en Sistemas Computarizados

P R E S E N T A

MARCO ANTONIO BARRERA ARGÜELLO

A S E S O R

M. en A. Sergio Francisco Barraza Ibarra

Clave: 16PSU0014Q

Acuerdo: 952006

MORELIA, MICH.

OCTUBRE 2001

DEDICATORIA.

PRIMERAMENTE A TODOS LO QUE YA NO ESTAN AQUÍ, MIS ABUELOS, MIS TIOS, MIS AMIGOS, QUE NO LE FUE POSIBLE COMPARTIR ESTE MOMENTO CONMIGO, PERO QUE MUCHO ME HA SERVIDO LO QUE VIVIMOS JUNTOS, GRACIAS.

A MIS PADRES QUE CON ESTA CULMINACION SE VE RECOMPENSADO TODO SUS ESFUERZOS, CORAJES Y SACRIFICIOS DE UNA FORMA MINIMA, GRACIAS POR SER MIS PAPAS.

A MIS TIOS: ESPERANZA, RAYMUNDO, GELA, ADRIAN, DORA, PADRINO LUIS, PACHITA +, FELIPE, CONSUELO, Y MAS, POR CADA UNO DE SUS CONSEJOS Y APOYOS QUE ME HAN DADO HAN SERVIDO DE ESTIMULO PARA SALIR MAS ADELANTE, GRACIAS POR ESOS MOMENTOS QUE NO OLVIDARE.

A MIS PRIMOS: MARCELA, LUPITA, RUBEN, ANGEL, JUDITH, MANOLO, TACHIN, ETC Y OTROS 48 PRIMOS MAS QUE MUCHO HAN SIGNIFICADO EN MI VIDA. GRACIAS POR SU CARÍÑO.

A LIZIE, ALBERTO, HECTOR, PACO, IVAN, ENRIQUE, DANIEL Y TODOS LOS DEMAS QUE SERIA TANTOS LE QUIERO AGRADECER TODOS LOS MOMENTOS QUE HEMOS VIVIDO TANTO AGRADABLE COMO TRISTES, SE LOS DEDICO COMO UN POCO DE LO MUCHO QUE ME HAN DADO.

A LIZ, POR QUE ME HAZ DADO UN NUEVO SENTIR POR LA VIDA, ESPERO CONTAR CONTIGO SIEMPRE...

POR ULTIMO A ESA PERSONA QUE HA COMPARTIDO DE SU CARÍÑO, Y SU TIEMPO CONMIGO, NO HAY FORMA DE AGRADECERTE TODO LO QUE HAS HECHO POR MI, GRACIAS CIELO.

PARA MI MISMO....

**¿QUE HE BUSCADO?
ESA ES UNA BUENA PREGUNTA
HE TRATADO MUCHAS VECES
DE BUSCAR A DIOS
Y A LA JUSTICIA.
SOY UN POBRE DIABLO
QUE ANDA ENTRE
EL CIELO Y EL INFIERNO.
SOY UNA GENTE
QUE LO QUIERE TODO
Y QUE NO HA ALCANZADO NADA.
DURANTE DIAS, MESES O AÑOS,
BUSCO
LA JUSTICIA, EL PAN, LA SAL,
EL AMOR Y LA MUJER,
Y HAY MOMENTOS,
BREVES MOMENTOS,
EN QUE HE QUERIDO BUSCARLO
Y TALVEZ NUNCA LO HE ENCONTRADO
EL DIA QUE LO ENCUENTRE...
ME QUEDARE CALLADO.**

NP.

INDICE

1.- INTRODUCCION.....	1
2.- OBJETIVOS GENERALES Y ESPECIFICOS.....	3
3.- INTRODUCCION A REDES LOCALES.....	5
3.1.- CONCEPTOS BASICOS DE COMUNICACIÓN DE DATOS.....	6
3.2.- MEDIOS, FORMAS Y TIPOS DE TRANSMISION.....	7
3.3.- MODEMS COMO DISPOSITIVO DE COMUNICACIÓN.....	9
3.4.- ¿QUE ES UNA RED?.....	10
3.5.- RED DE AREA LOCAL Y SUS COMPONENTES.....	10
3.5.1.- SERVIDORES O FILE SERVERS.....	11
3.5.2.- ESTACIONES DE TRABAJO.....	13
3.5.3.- TARJETA DE RED O NIC(NETWORK INTERFACE CARD) ETHERTNET.....	13
3.5.4.- CONECTORES Y TARJETAS DE RED LOCAL TALK.....	14
3.5.5.- CONCENTRADORES O HUB 'S.....	15
3.5.6.- REPETIDORES.....	16
3.5.7.- BRIDGES O PUENTES.....	17
3.5.8.- ROUTERS O RUTEADORES.....	17
3.5.9.- FIREWALLS O CORTAFUEGOS.....	18
4.- EL MODELO DE REDES OSI.....	21
4.1.- EL NIVEL FISICO.....	22
4.1.1.- MEDIOS DE TRANSMISION.....	23
4.2.- EL NIVEL DE ENLACE DE DATOS.....	25
4.3.- EL NIVEL DE RED.....	25
4.4.- EL NIVEL DE TRANSPORTE.....	28
4.4.1.- PROTOCOLOS DE TRANSPORTE.....	28
4.5.- EL NIVEL DE APLICACIÓN.....	31
5.- EL CABLEADO DE UNA RED Y SUS CARACTERISTICAS.....	34
5.1.- CABLE DE PAR TRENZADO SIN APANTALLAR.....	34
5.1.1.- CATEGORIAS UTP.....	35
5.1.2.- CONECTOR UTP.....	36
5.2.- CABLE DE PAR TRENZADO PANTALLADO.....	36
5.3.- CABLE COAXIAL.....	37
5.3.1.- CONECTOR PARA CABLE COAXIAL.....	38
5.4.- CABLE DE FIBRA OPTICA.....	38
5.4.1.- CONECTOR PARA FIBRA OPTICA.....	39
5.5.- RESUMEN DE TIPOS DE CABLE.....	40
5.6.- REDES LOCALES SIN CABLEADO.....	40

6. - TOPOLOGIAS Y PROTOCOLOS DE UNA RED LOCAL.....	41
6.1. - TOPOLOGIA DE BUS /LINEAR BUS.....	41
6.1.1. - VENTAJAS Y DESVENTAJAS.....	42
6.2. - TOPOLOGIA DE ESTRELLA/STAR.....	42
6.2.1. - VENTAJAS Y DESVENTAJAS.....	43
6.3. - TOPOLOGIA DE ESTRELLA CABLEADA/STAR-WIRED RING.....	44
6.4. - TOPOLOGIA DE ARBOL/TREE.....	44
6.4.1. - VENTAJAS Y DESVENTAJAS.....	45
6.5. - PROTOCOLOS EN REDES LOCALES.....	46
6.5.1. - ETHERNET.....	47
6.5.2. - LOCALTALK.....	50
6.5.3. - TOKEN RING.....	51
6.5.4. - F D D I	52
6.6. - RESUMEN DE PROTOCOLOS.....	54
7. - ETAPAS DE UN RED LOCAL.....	55
7.1. - ASPECTOS GENERALES.....	55
7.2. - PRIMERA ETAPA: DISEÑO DE UNA RED LOCAL.....	57
7.3. - SEGUNDA ETAPA: IMPLEMENTACION Y VALIDACION.....	60
8. - REDES LOCALES EN MS WINDOWS 95/98/MILLENIUM.....	66
8.1. - PRINCIPALES COMPONENTES.....	67
8.2. - METODOS DE COMUNICACIÓN.....	70
8.3. - PROTOCOLOS IP Y ARP.....	70
8.4. - CLIENTE PARA REDES	75
8.5. - GRUPO DE TRABAJO.....	77
8.6. - TIPOS DE CONTRASEÑA.....	79
8.7. - INSTALACION DE RECURSOS COMPARTIDOS.....	80
8.9. - MONITORIZACION DE LA RED.....	82
8.10. - COMPARTIR UNA SOLA CONEXIÓN A INTERNET.....	85
8.11. - CONCLUSIONES.....	89
9. - ADMINISTRACION Y CONFIGURACION DE WINDOWS NT.....	90
9.1. - INTRODUCCION A WINDOWS NT.....	90
9.2. - DESCRIPCION GENERAL.....	91
9.3. - ARQUITECTURA DE REDES ABIERTAS.....	91
9.4. - REGISTRO DE CONFIGURACION.....	93
9.5. - VENTAJAS Y DESVENTAJAS DE WINDOWS NT.....	95
9.6. - PRINCIPALES CARACTERISTICAS.....	97
9.7. - FUNCIONAMIENTO DE LA SEGURIDAD EN RED.....	99
9.8. - DOMINIOS Y RELACION DE CONFIANZA.....	105
9.9. - ARQUITECTURA DEL SISTEMA.....	108

10.- ADMINISTRACION Y CONFIGURACION EN WINDOWS 2000.....	115
10.1. – COMO ES WINDOWS 2000.....	115
10.2. – CUALES SON MEJORAS	115
10.3. – QUE VERSIONES VIENE EL WINDOWS 2000.....	115
10.4. – REQUERIMIENTOS TECNICOS.....	116
10.5. – INSTALACION.....	116
10.6. – TIPO DE SOPORTE DE HARDWARE.....	117
10.7. – CAMBIOS GRAFICOS.....	118
10.8. – NOVEDADES DE LA INTERFAZ.....	118
10.9. – FACILIDADES DE USO.....	119
10.10. – PANTALAS AZULES EN ESTA VERSION.....	119
10.11. – FIABILIDAD.....	120
10.12. – GESTION DEL SISTEMA.....	120
10.13. – SEGURIDAD DEL SISTEMA.....	121
10.14. – ACTIVE DIRECTORY.....	122
10.15. – WINDOWS 2000 EN PC´S PORTATILES.....	123
10.16. – CONFIGURACION DE ACCESO A INTERNET.....	124
10.17. – RED PRIVADA VIRTUAL (VPN).....	129
11. – WINDOWS XP Y WHISTLER S.O. MAS ESPERADO.....	134
11.1. – INTRODUCCION.....	134
11.2. – VERSIONES PRELIMINARES.....	134
11.3. – VERSIONES.....	134
11.4. – NOVEDADES DE LA INTERFAZ.....	135
11.5. – CAMBIO E INICIO RAPIDO DE USUARIOS.....	135
11.6. – MENU DE INICIO Y BARRA DE TAREAS.....	136
11.7. – MULTIMEDIA.....	137
11.8. – TRABAJANDO CON IMÁGENES.....	138
11.9. – MULTIMEDIA.....	138
11.10. – LA NUEVA CARA DE LA MUSICA.....	140
11.11. – INTERNET.....	141
11.12. – FIABILIDAD, SEGURIDAD Y ROBUSTEZ.....	142
11.13. – ASISTENCIA REMOTA.....	142
11.14. – CORTAFUEGOS (FIREWALL).....	143
11.15. – RESTAURAR EL SISTEMA.....	143
11.16. – DRIVERS.....	144

12. – TRUCOS, RECOMENDACIONES Y ALGO MAS DE REDES LOCALES.....	145
12.1. ENCONTRAR UNA PC EN LA RED.....	145
12.2. UNA RED CON UN CD ROM.....	145
12.3. BUSCAR UNA PC EN LA RED.....	145
12.4. BUSCAR UNA PC EN LA RED (2).....	146
12.5. CREAR DISCO DE INICIO CON PROTOCOLO NETBEUI.....	146
12.6. CONECTAR 2 PC ´S CON CABLE UTP SIN CONCENTRADOR.....	147
12.7. CONECTAR UNA PC C/ DOS CON UNA WINDOWS 95/98.....	148
12.8. CONECTAR VARIOS PC ´S A UNA RED.....	150
12.9. IDENTIFICAR UN USUARIO DE UNA MAQUINA.....	152
12.10. CONECTAR VARIAS IMPRESORAS NETPORT O JECTDIRECT.....	151
12.11. SINCRONIZAR LOS RELOJES DE LAS PC ´S EN UNA RED.....	152
12.12. ENVIAR MENSAJES ENTRE TERMINALES DE UNA RED.....	153
12.13. JUGAR EN RED SIN ENTRAR A WINDOWS.....	153
12.14. ACELERAR CONEXIONES A RED.....	154
12.15. ADMINISTRAR UN PC WIN95 DESDE OTRO PC SIN TENER SHARED.....	155
12.16. DIFERENCIA ENTRE PROTOCOLO NETBEUI Y TCP/IP.....	156
12.17. UTILIZAR LAS MISMAS BASES DE MENSAJES OUTLOOK EN TODOS LAS TERMINALES.....	156
12.18. ENVIAR Y RECIBIR MENSAJES CON SAMBAR.....	157
12.19. COMO HACER UN TERMINADOR IMPROVISADO.....	158
12.20. CONCLUSIONES DEL CAPITULO.....	158
13. – RECOMENDACIONES.....	159
14. – CONCLUSIONES.....	161
15. – ACRONIMOS GENERALES.....	163
16. – GLOSARIO.....	168
17. – BIBLOGRAFIA.....	187

1.- INTRODUCCION.

La tecnología digital esta transformando la forma en que se ha ce los negocios al igual que los roles que desempeñan los trabajadores en sus empresas. La permanencia y proyección de las diferentes compañías, va a depender de la velocidad con que se adapten a este cambio, para lo cual deberán contar con la infraestructura adecuada para procesar en e forma eficiente toda su información.

La base para el éxito de cualquier sistema de información digital es tener una arquitectura sólida, capaz de proveer los servicios necesarios para soportar el procesamiento de grandes volúmenes de información de modo que este disponible en el momento adecuado para la persona indicada.

El estudio de redes de cómputo comprende un campo un campo bastante amplio, ya que enfatizar en un todo lo correspondiente a la parte de redes de computadoras es complejo debido al constante desarrollo que en este campo se da cada vez con más y mejores características relacionadas con herramientas administrativas del sistema. Es esta parte de la administración la que requiere de estudio y disponibilidad de tiempo, por tanto el proyecto abarcara en la parte teórica los aspectos más importantes de la tecnología actual en diseño e implementación en redes.

El Internet es un notable avance en la conquista del software de redes, potente y sólido, puede adecuarse a diferentes equipos y usuarios.

En redes no existe algo estándar o definido, a cualquier decisión, le podemos encontrar limites, puesto que no existe un sistema operativo establecido para lo que es redes, todo se encuentran en proceso.

Las redes tienden a crecer e innovarse, al principio se conectan unas cuantas personas y luego todo el mundo desea conectarse, hasta verse en la necesidad de conectarse a un correo electrónico.

Tal parece que la comunicación es una actividad de primera necesidad actualmente, y esto da como resultado el gran adelanto tecnológico constante y arduo en e campo de telecomunicaciones.

Este trabajo es el resultado de la experiencia desarrollada a lo largo de 4 años trabajando con redes locales en diferentes versiones de sistemas operativos de Microsoft, con diferentes capacidades de equipos y adecuándose a alas necesidades, explicando de forma grafica todo su contenido lo cual hace su entendimiento mas fácil, brindando en el un fuente de consulta y de aplicaciones reales para situaciones del mundo real.

2.- OBJETIVOS GENERALES Y ESPECIFICOS.

OBJETIVOS GENERALES.-

ESTE TRABAJO TIENE COMO PRINCIPAL OBJETIVO SABER DIFERENCIAR LAS NECESIDADES REALES DE UN RED LOCAL, ASI COMO CONOCER LAS VENTAJAS Y DESVENTAJAS DE TODOS LOS SISTEMAS OPERATIVOS DE MICOSOFT, CARACTERISTICAS, POSIBILIDADES Y LIMITANTES TANTO DE HARDWARE COMO DE SOFTWARE.

OBJETIVOS ESPECIFICOS.-

- CONOCER LOS CONCEPTOS BASICOS DE UNA RED LOCAL Y MEDIOS DE TRANSMISION.
- DEFINIR LOS NIVELES DEL MODELO OSI QUE SE UTILIZAN EN UNA RED LOCAL.
- IDENTIFICAR LOS DIFERENTES TIPO DE CABLEADO ASI COMO SUS CARACTERISTICAS.
- DESCRIBIR LOS PROTOCOLOS Y TOPOLOGIAS DE UNA RED LOCAL CONOCIENDO SUS VENTAJAS Y DESVENTAJAS.
- CITAR LOS DIFERENTES PASOS QUE SE DEBEN SEGUIR PARA LA CONSTRUCCION DE UNA RED LOCAL.
- DETALLAR LAS PRINCIPALES CARACTERISTICAS DE LOS SISTEMAS OPERATIVOS.
- APRENDER LA CONFIGURACION DE UNA RED LOCAL BAJO LOS SISTEMAS OPERATIVOS DE MICROSOFT.
- DESCRIBIR COMO COMPARTIR RECURSOS Y DISPOSITIVOS EN RED

- MOSTRAR LAS FORMAS DE TENER UNA RED LOCAL SEGURA.
- RESALTAR LA EVOLUCION Y LAS MEJORAS QUE HA SUFRIDO A LO LARGO QUE HAN SIDO CREADOS.
- MANEJAR LAS DIFERENTES INTERFAZ DE CADA UNO DE LOS SISTEMAS OPERATIVOS
- CONOCER LOS DIFERENTES TRUCOS, RECOMENDACIONES Y PRINCIPIOS PARA TENER UNA RED EN OPTIMO ESTADO.

3.- INTRODUCCIÓN A LAS REDES LOCALES .

Con el desarrollo del proyecto se ha creado una herramienta de consulta accesible y clara, para quienes tengan un mínimo conocimiento de instalación de redes y también para aquellas personas que quieran ahondar en conocimientos ya adquiridos.

Con todos estos requerimientos damos a conocer el presente proyecto, esperando que en el, se encuentre una fuente de consulta que se adecue a las necesidades de los usuarios.

Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, CD-Roms o impresoras y que son capaces de realizar comunicaciones electrónicas. Las redes están unidas por cable, líneas de teléfono, ondas de radio, satélite, etc.

Su objetivo principal es lograr que todos sus programas datos y equipo estén disponible para cualquiera de la red que lo solicite, sin importar la localización física del recurso y del usuario.

Otro de sus objetivos consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, es decir que todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Igualmente la presencia de varios CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque su rendimiento en general sea menor.

El ahorro económico debido a que los ordenadores pequeños tiene una mejor relación costo / rendimiento, en comparación con la que ofrece las máquinas grandes.

Proporciona un poderoso medio de comunicación entre personas que se encuentran en lugares distantes entre sí.

CONCEPTOS BASICOS DE COMUNICACION DE DATOS

Comunicación de Datos. Es el proceso de comunicar información en forma binaria entre dos o más puntos. Requiere cuatro elementos básicos que son:

Emisor: Dispositivo que transmite los datos

Mensaje: lo conforman los datos a ser transmitidos

Medio : consiste en el recorrido de los datos desde el origen hasta su destino

Receptor: dispositivo de destino de los datos

BIT: es la unidad más pequeña de información y la unidad base en comunicaciones.

BYTE: conjunto de bits continuos mínimos que hacen posible, un direccionamiento de información en un sistema computarizado. Está formado por 8 bits.

Trama : tira de bits con un formato predefinido usado en protocolos orientados a bit.

Paquete : fracciones de un mensaje de tamaño predefinido, donde cada fracción o paquete contiene información de procedencia y de destino, así como información requerida para el reensamblado del mensaje.

Interfaces: conexión que permite la comunicación entre dos o más dispositivos.

Códigos: acuerdo previo sobre un conjunto de significados que definen una serie de símbolos y caracteres. Toda combinación de bits representa un carácter dentro de la tabla de códigos. las tablas de códigos más reconocidas son las del código ASCII y la del código EBCDIC.

Modulación: proceso de manipular de manera controlada las propiedades de una señal portadora para que contenga la información que se va a transmitir

MEDIOS , FORMAS Y TIPOS DE TRANSMISION

Medios

Aéreos: basados en señales radio-eléctricas (utilizan la atmósfera como medio de transmisión), en señales de rayos láser o rayos infrarrojos.

Sólidos: principalmente el cobre en par trenzado o cable coaxial y la fibra óptica.

Formas

Transmisión en Serie: los bits se transmiten de uno a uno sobre una línea única. Se utiliza para transmitir a larga distancia.

Transmisión en Paralelo: los bits se transmiten en grupo sobre varias líneas al mismo tiempo. Es utilizada dentro del computador.

La transmisión en paralela es más rápida que la transmisión en serie pero en la medida que la distancia entre equipos se incrementa (no debe sobrepasarse la distancia de 100 pies), no solo se encarecen los cables sino que además aumenta la complejidad de los transmisores y los receptores de la línea a causa de la dificultad de transmitir y recibir señales de pulsos a través de cables largos.

Tipos

Transmisión Simplex: la transmisión de datos se produce en un solo sentido. siempre existen un nodo emisor y un nodo receptor que no cambian sus funciones.

Transmisión Half-Duplex: la transmisión de los datos se produce en ambos sentidos pero alternativamente, en un solo sentido a la vez. Si se está recibiendo datos no se puede transmitir.

Transmisión Full-Duplex: la transmisión de los datos se produce en ambos sentidos al mismo tiempo. un extremo que esta recibiendo datos puede, al mismo tiempo, estar transmitiendo otros datos.

Transmisión Asíncrona: cada byte de datos incluye señales de arranque y parada al principio y al final. La misión de estas señales consiste en:

- Avisar al receptor de que está llegando un dato.
- Darle suficiente tiempo al receptor de realizar funciones de sincronismo antes de que llegue el siguiente byte.

Transmisión Síncrona: se utilizan canales separados de reloj que administran la recepción y transmisión de los datos. Al inicio de cada transmisión se emplean unas señales preliminares llamadas:

- Bytes de sincronización en los protocolos orientados a byte.
- Flags en los protocolos orientados a bit.

Su misión principal es alertar al receptor de la llegada de los datos.

Nota: Las señales de reloj determinan la velocidad a la cual se transmite o recibe.

MODEMS

Un Módem es un dispositivo que convierte la señal digital en señal analógica y viceversa para posibilitar que el mensaje enviado por un DTE pueda llegar a otro(s) DTE's a través de líneas análogas.

Los Modems podemos seleccionarlos de acuerdo a:

1. La velocidad de transmisión
2. El tipo de línea que utiliza: dedicada, conmutada o ambas.
3. La modulación que emplea: FSK, PSK, DPSK, QAM, TCM.
4. Las posibilidades de compresión de datos para transmisión.
5. La modalidad de trabajo: punto a punto o Multipunto.
6. Si se instala interno o externo al equipo DTE.

En la practica el mercado de los módems crea dos grupos:

Modems empleados en centros de transmisión con una permanente o casi permanente actividad, las cuales cuentan con mecanismos sofisticados de diagnostico, control y administración centralizados y remotos.

Modems de Escritorios cuyo principal uso es la conexión a través de la red pública telefónica, con cierta regularidad pero nunca con carácter permanente ni con uso exhaustivo.

Multiplexor por División de Tiempo Estadísticos: no le ofrece ranuras de tiempo a los canales inactivos y además podemos asignar prioridades a los canales.

PRINCIPALES COMPONENTES DE LAS REDES LOCALES

¿Qué es una red?

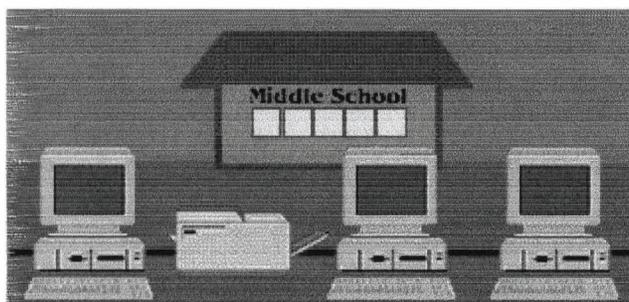
Una red consiste en dos o más computadoras unidas que comparten recursos (ya sea archivos, CD-ROM's o impresoras) y que son capaces de realizar comunicaciones electrónicas. Las redes pueden estar unidas por cable, líneas de teléfono, ondas de radio, satélites, infrarrojos, etc...

La clasificación básica de redes es:

- Red de Area Local / Local Area Network (LAN)
- Red de Area Metropolitana / Metropolitan Area Network (MAN)
- Red de Area Extensa / Wide Area Network (WAN)

Red de área Local / Local Area Network (LAN)

Se trata de una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc... No habrá por lo general dos ordenadores que disten entre sí más de un kilómetro.



Una configuración típica en una red de área local es tener una computadora llamada servidor de ficheros en la que se almacena todo el software de control de la red así como el software que se comparte con los demás ordenadores de la red. Los ordenadores que no son servidores de ficheros reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y suelen tener software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

Las redes de ordenadores se montan con una serie de componentes de uso común y que en mayor o menor medida siempre aparecerán en cualquier instalación.

Comentaremos:

- Servidores o File servers
- Estaciones de trabajo o Workstations
- Tarjetas de Red (NIC)
- Concentradores y Hubs
- Repetidores
- Puentes o Bridges
- Routers
- Cortafuegos o Firewalls

Servidores

Los servidores de ficheros conforman el corazón de la mayoría de las redes. Se trata de ordenadores con mucha memoria RAM, un enorme disco duro (o varios) y una rápida tarjeta de red. El sistema operativo de red se ejecuta sobre estos servidores así como las aplicaciones compartidas.

Un servidor de impresión se encargará de controlar gran parte del tráfico de red ya que será el que acceda a las demandas de las estaciones de trabajo, y el que les proporcione los servicios que pidan, impresión, ficheros, Internet, etc...

Está claro que necesitamos un ordenador con capacidad de guardar información de forma muy rápida y de compartirla con la misma celeridad.

Por último, cabría señalar que existen distintas clases de servidores de ficheros:

- **Servidores genéricos.** Son usualmente mini o microordenadores estándar. Se suelen usar PC's o estaciones RISC. Los servidores genéricos son a menudo más flexibles que los servidores propietarios, y fáciles de reconvertir en estaciones de trabajo si quedaran obsoletos.
- **Servidores propietarios.** Son máquinas diseñadas especialmente para usarse como servidores de red. Ofrecen un mayor rendimiento que los servidores genéricos ya que proporcionan una serie de funciones extra. Su desventaja es que sólo soportan normalmente un único sistema operativo de red, para el que han sido optimizados.
- **Servidores no-dedicados.** Trabajan para el usuario como estaciones de trabajo o como servidores de ficheros. El rendimiento y la integridad del sistema pueden ser un riesgo a la hora de decidirse por esta solución ya que las aplicaciones y los usuarios que estén trabajando en el servidor se pueden bloquear por completo, aunque una ventaja es el ahorro de una estación de trabajo.
- **Servidores dedicados.** Funcionan estrictamente como servidores, no estando disponibles como estaciones de trabajo. Proporcionan mucho mejor rendimiento y seguridad e integridad del sistema que los anteriores.
- **Servidores de impresora.** Hay sistemas operativos de red que permiten configurar un ordenador como servidor de impresora, este ordenador sería el encargado de gestionar el directorio de *spooling*, que funciona como una cola FIFO a la cual llegan los trabajos para su impresión.
- **Servidores de fax.** Proporcionan a todas las estaciones de la red acceso a un servicio fax ejecutándose en el servidor, que puede ser un ordenador con tarjeta de fax o un dispositivo especial diseñado para este fin.

Estaciones de trabajo

Son los ordenadores conectados al servidor. Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesitan una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Una estación de trabajo puede carecer de disquete y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier ordenador puede actuar como una estación de trabajo.

Tarjeta de Red

La tarjeta de red (NIC) es la que conecta físicamente al ordenador a la red. Son tarjetas que se pinchan en el ordenador como si de una tarjeta de video se tratase o cualquier otra tarjeta. Puesto que todos los accesos a red se realizan a través de ellas se deben utilizar tarjetas rápidas si queremos comunicaciones fluidas.

Las tarjetas de red más populares son por supuesto las tarjetas Ethernet, existen también conectores LocalTalk así como tarjetas TokenRing.

Tarjetas Ethernet

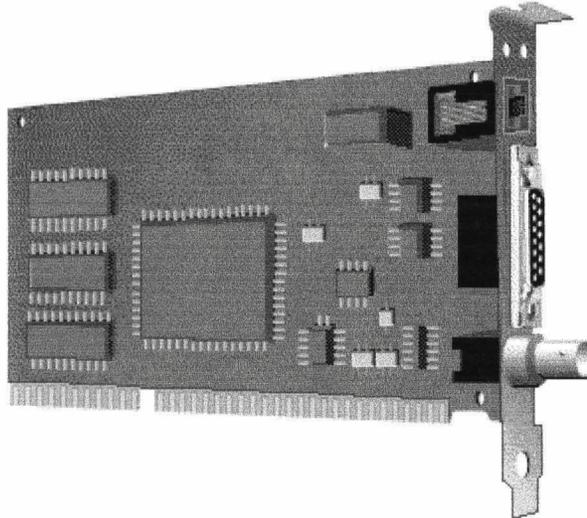
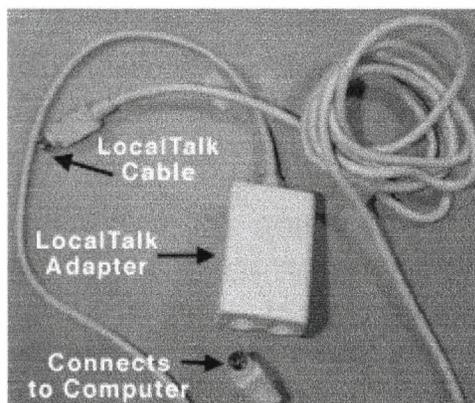


Fig. 1. Tarjeta Ethernet con conectores RJ-45, AUI, BNC

Conectores LocalTalk

Se utilizan para ordenadores Mac, conectándose al puerto paralelo. En comparación con Ethernet la velocidad es muy baja, de 230KB frente a los 10 o 100 MB de la primera.

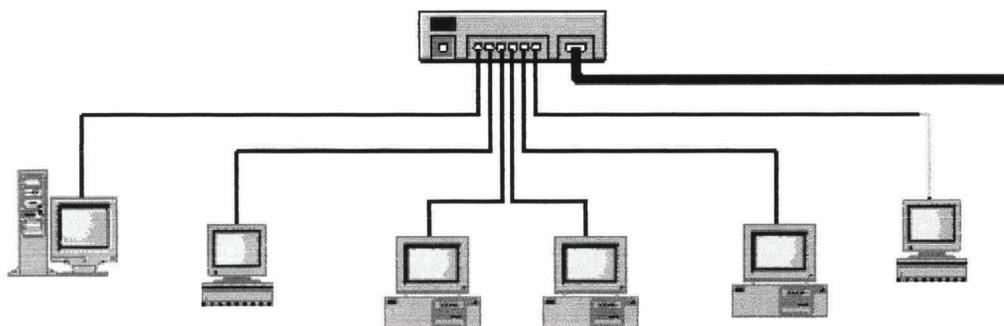
Un ejemplo de como son los conectores LocalTalk.



Tarjetas Token Ring

Son similares a las tarjetas Ethernet aunque el conector es diferente. Suele ser un DIN de nueve pines.

Concentradores o Hubs

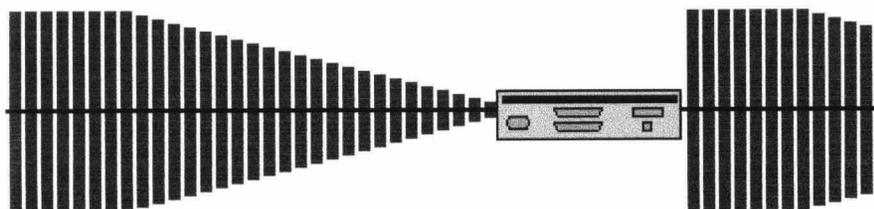


Un concentrador o Hub es un elemento que provee una conexión central para todos los cables de la red. Los hubs son "cajas" con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red.

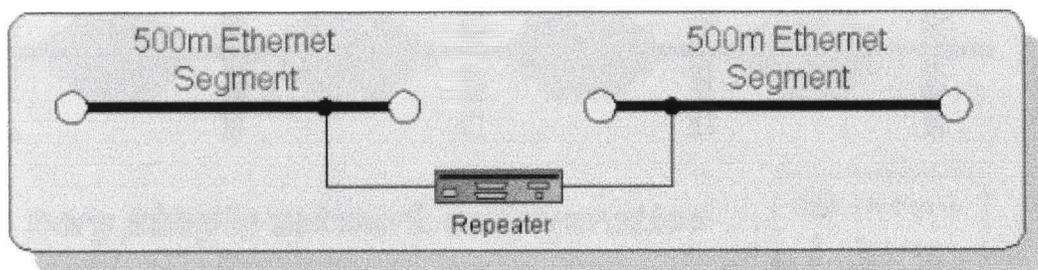
Los hay de tipo inteligente que envían la información solo a quien ha de llegar mientras que los normales envían la información a todos los puntos de la red siendo las estaciones de trabajo las que decidirán si se quedan o no con esa información.

Están provistos de salidas especiales para conectar otro Hub a uno de los conectores permitiendo así ampliaciones de la red.

Repetidores



Cuando una señal viaja a lo largo de un cable va perdiendo "fuerza" a medida que avanza. Esta pérdida de fuerza puede desembocar en una pérdida de información. Los repetidores amplifican la señal que reciben permitiendo así que la distancia entre dos puntos de la red sea mayor que la que un cable solo permite.



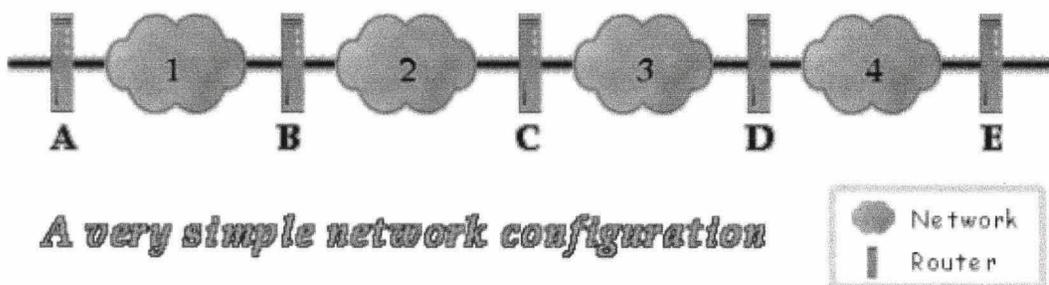
Esto es que cuando la especificación técnicas del medio es menor que la distancia por cubrir, se requiere de un repetidor, como nos indica la grafica donde unimos dos segmentos de 500 mts cada uno.

Bridges

Los bridges se utilizan para segmentar redes grandes en redes más pequeñas. De esta forma solo saldrá de la red pequeña el tráfico destinado a otra red pequeña diferente mientras que todo el tráfico interno seguirá en la misma red. Con esto se consigue una reducción del tráfico de red.

Routers

Un router dirige tráfico de una red a otra, se podría decir que es un bridge superinteligente ya que es capaz de calcular cual será el destino más rápido para hacer llegar la información de un punto a otro. Es capaz también de asignar diferentes preferencias a los mensajes que fluyen por la red y enrutar unos por caminos más cortos que otros así como de buscar soluciones alternativas cuando un camino está muy cargado.



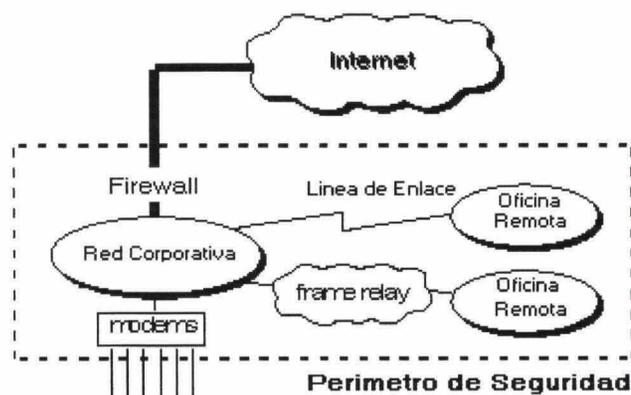
Mientras un bridge conoce la dirección de las computadoras a cada uno de sus extremos un router conoce la dirección tanto de las computadoras como de otros routers y bridges y es capaz de "escanear" toda la red para encontrar el camino menos congestionado.

Cortafuegos o Firewalls

Un firewall es un elemento de seguridad que filtra el tráfico de red que a él llega. Con un cortafuegos podemos aislar un ordenador de todos los otros ordenadores de la red excepto de uno o varios que son los que nos interesa que puedan comunicarse con él.

El firewall determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

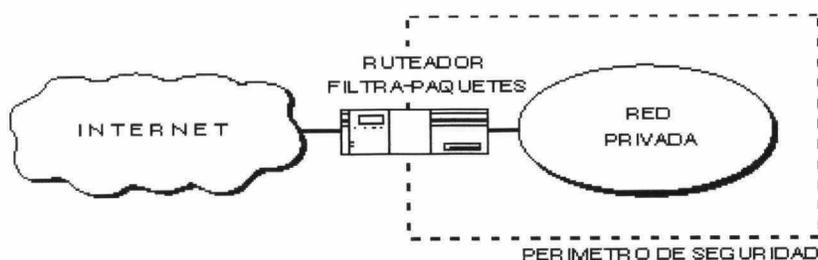
Regularmente se utiliza para proteccion de internet, ya que muchas veces con la ayuda de programas puedes entrar a red locales de empresas con acceso a internet desde el mismo internet.



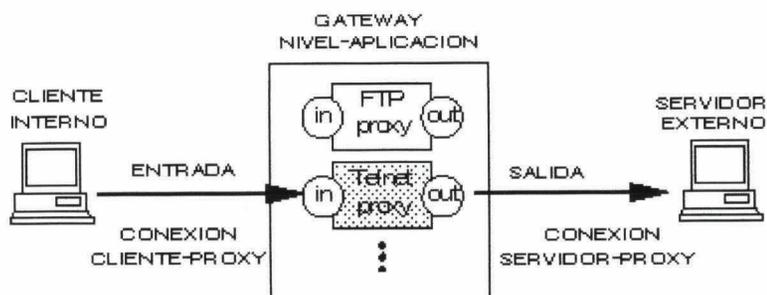
En la figura se ve como el cortafuegos se instala en la parte por donde pasa todos los usuarios o por donde se tiene acceso al exterior.

Después de las decisiones acerca de los ejemplos previos, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Ruteador Filtra-paquetes.
Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos.

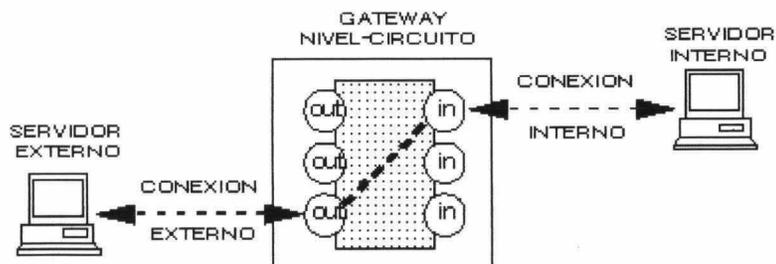


- Gateway a Nivel-aplicación.
Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes.



- Gateway a Nivel-circuito.

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.



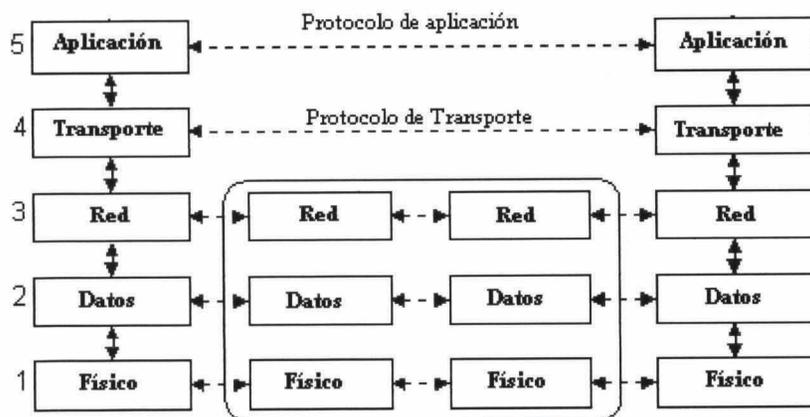
4. - El modelo de Redes OSI

Aunque al final a nosotros nos parezca sencillo, conectar en red dos equipos es un complicado problema de ingeniería. Cuando se abordan problemas de esta magnitud, la forma de solucionarlos suele ser dividir el problema grande en problemas pequeños. Esto es lo que propone el modelo de redes *OSI* (OPEC Sistema Interconnection), publicado por la organización internacional ISO. Este modelo divide el "gran problema" en 7 pequeños problemas a los que se conoce como los siete niveles de red OSI.

Veamos los siete niveles:

- 1) **Físico:** Conecta físicamente a dos transmisores
- 2) **Datos:** Controla posibles errores entre dos puntos
- 3) **Red:** Encamina la información a través de la red
- 4) **Transporte:** Propicia la comunicación entre dos puntos no adyacentes
- 5) **Sesión:** Gestiona problemas ajenos a la comunicación
- 6) **Presentación:** Convierte la información
- 7) **Aplicación:** Proporciona servicios a las aplicaciones

Estos siete niveles se pueden reagrupar en una variante de 5 donde el nivel aplicación engloba a los niveles 5 y 6



El nivel físico

El nivel físico viene a ser básicamente el "cable" que permite la comunicación y transmisión de datos, y que define la transmisión de bits a través de un canal. Esto quiere decir que se ha de asegurar que cuando un punto de la comunicación envía un bit 1, este se reciba como un bit 1, no como un bit 0. Las cuestiones que se tratarán será como cuantos voltios representan el 1, cuantos el 0, cuantos microsegundos dura un bit, si la transmisión se puede efectuar en los dos sentidos del canal, como se inicia una conexión, como se acaba, cuantos pins deben tener los conectores de red y que señal transporta cada uno de ellos.

En esta capa se tratan conceptos mecánicos eléctricos, y procedimientos de interfase así como el medio de transmisión.

Medios de transmisión

- **Par trenzado (*twisted pair*).** Consiste en dos alambres de cobre enroscados (para reducir interferencia eléctrica).
- **Cable coaxial.** Un alambre dentro de un conductor cilíndrico. Tiene un mejor blindaje y puede cruzar distancias mayores con velocidades mayores
- **Fibra óptica.** Hoy tiene un ancho de banda de 50.000 Gbps, pero es limitada por la conversión entre las señales ópticas y eléctricas (1 Gbps). Los pulsos de luz rebotan dentro de la fibra.

Además de estos hay también medios inalámbricos de transmisión. Cada uno usa una banda de frecuencias en alguna parte del espectro electromagnético. Las ondas de longitudes más cortas tienen frecuencias más altas, y así apoyan velocidades más altas de transmisión de datos. Veamos algunos ejemplos:

- **Radio.** 10 KHz-100 MHz. Las ondas de radio son fáciles de generar, pueden cruzar distancias largas, y entrar fácilmente en los edificios. Son omnidireccionales, lo cual implica que los transmisores y receptores no tienen que ser alineados.
 - Las ondas de frecuencias bajas pasan por los obstáculos, pero el poder disminuye con la distancia.
 - Las ondas de frecuencias más altas van en líneas rectas. Rebotan en los obstáculos y la lluvia las absorbe.
- **Microondas.** 100 MHz-10 GHz. Van en líneas rectas. Antes de la fibra formaban el centro del sistema telefónico de larga distancia. La lluvia las absorbe.
- **Infrarrojo.** Se usan en la comunicación de corta distancia (por ejemplo, control remoto de televisores). No pasan por las paredes, lo que implica que sistemas en distintas habitaciones no se interfieren. No se pueden usar fuera.
- **Ondas de luz.** Se usan lasers. Ofrecen un ancho de banda alto con costo bajo, pero el rayo es muy angosto, y el alineamiento es difícil.

El sistema telefónico

- En general hay que usarlo para redes más grandes que un LAN.
- Consiste en las oficinas de conmutación, los alambres entre los clientes y las oficinas (los *local loops*), y los alambres de las conexiones de larga distancia entre las oficinas (los *troncales*). Hay una jerarquía de las oficinas.
- La tendencia es hacia la señalización digital. Ventajas:
 - La regeneración de la señal es fácil sobre distancias largas.
 - Se pueden entremezclar la voz y los datos.
 - Los amplificadores son más baratos porque solamente tienen que distinguir entre dos niveles.
 - La manutención es más fácil; es fácil detectar errores.

Satélites

- Funcionan como repetidores de microondas. Un satélite contiene algunos transpondedores que reciben las señales de alguna porción del espectro, las amplifican, y las retransmiten en otra frecuencia.
- Hay tres bandas principales: C (que tiene problemas de interferencia terrenal), Ku, y Ka (que tienen problemas con la lluvia).
- Un satélite tiene 12-20 transpondedores, cada uno con un ancho de banda de 36-50 MHz. Una velocidad de transmisión de 50 Mbps es típica. Se usa la multiplexación de división de tiempo.
- La altitud de 36.000 Km. sobre el ecuador permite la órbita geosíncrona, pero no se pueden ubicar los satélites con espacios de menos de 1 o 2 grados.
- Los tiempos de tránsito de 250-300 milisegundos son típicos.
- Muy útil en la comunicación móvil, y la comunicación en las áreas con el terreno difícil o la infraestructura débil.

El nivel de enlace de datos

El tema principal son los algoritmos para la comunicación confiable y eficiente entre dos máquinas adyacentes. Problemas: los errores en los circuitos de comunicación, sus velocidades finitas de transmisión, y el tiempo de propagación.

Marcos

El nivel de enlace trata de detectar y corregir los errores. Normalmente se parte el flujo de bits en *marcos* y se calcula un checksum (comprobación de datos) para cada uno.

Las tramas contendrán información como:

- **Número de caracteres** (un campo del encabezamiento guarda el número. Pero si el número es cambiado en una transmisión, es difícil recuperar.)

- **Caracteres de inicio y fin.**

Servicios para el nivel de red

Servicio sin acuses de recibo. La máquina de fuente manda marcos al destino. Es apropiado si la frecuencia de errores es muy baja o el tráfico es de tiempo real (por ejemplo, voz).

Servicio con acuses de recibo. El receptor manda un acuse de recibo al remitente para cada marco recibido.

Control de flujo

Se usan protocolos que prohíben que el remitente pueda mandar marcos sin la permisión implícita o explícita del receptor. Por ejemplo, el remitente puede mandar un número indeterminado de marcos pero entonces tiene que esperar.

Detección y corrección de errores

Ejemplo: HDLC

En este ejemplo se verá un protocolo que se podría identificar con el segundo nivel OSI. Es el HDLC (High-level Data Link Control). Este es un protocolo orientado a bit, es decir, sus especificaciones cubren que información lleva cada uno de los bits de la trama.

BITS 8	8	8	>=0	16	8
01111110	Address	Control	Datos	Checksum	01111110

Como se puede ver en la tabla, se definen unos campos que se agregan a la información (Datos). Estos campos se utilizan con distintos fines. Con el campo Checksum se detectan posibles errores en la transmisión mientras que con el campo control se envían mensajes como datos recibidos correctamente, etc...

El nivel de red

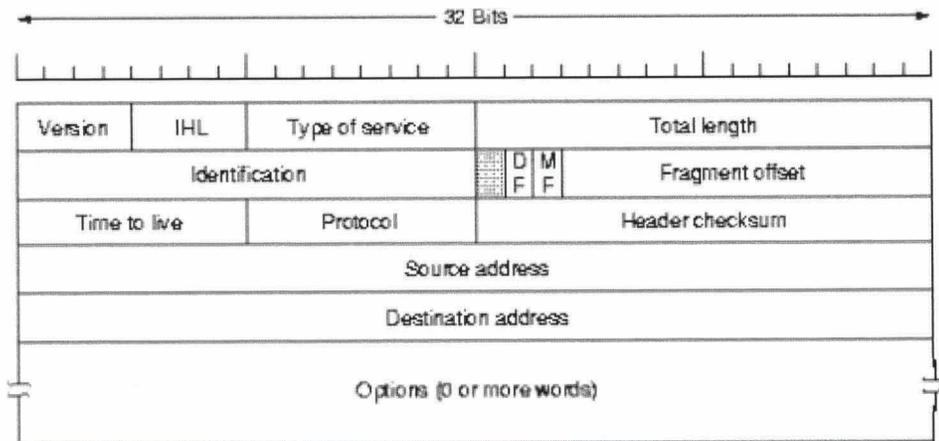
Este nivel encamina los paquetes de la fuente al destino final a través de encaminadores (routers) intermedios. Tiene que saber la topología de la subred, evitar la congestión, y manejar saltos cuando la fuente y el destino están en redes distintas.

El nivel de red en la Internet

Funcionamiento del protocolo IP

El protocolo de IP (Internet Protocol) es la base fundamental de Internet. Hace posible enviar datos de la fuente al destino. El nivel de transporte parte el flujo de datos en data gramas. Durante su transmisión se puede partir un data grama en fragmentos que se montan de nuevo en el destino.

Paquetes de IP:



- **Versión.** Es la 4. Permite las actualizaciones.
- **IHL.** La longitud del encabezamiento en palabras de 32 bits. El valor máximo es 15, o 60 bytes.
- **Tipo de servicio.** Determina si el envío y la velocidad de los datos es fiable. No usado.
- **Longitud total.** Hasta un máximo de 65.535 bytes.
- **Identificación.** Para determinar a qué datagrama pertenece un fragmento.
- **DF (Don't Fragment).** El destino no puede montar el datagrama de nuevo.
- **MF (More Fragments).** No establecido en el fragmento último.
- **Desplazamiento del fragmento.** A qué parte del datagrama pertenece este fragmento. El tamaño del fragmento elemental es 8 bytes.
- **Tiempo de vida.** Se decrementa cada salto.
- **Protocolo.** Protocolo de transporte en que se debiera basar el datagrama. Las opciones incluyen el enrutamiento estricto (se especifica la ruta completa), el enrutamiento suelto (se especifican solamente algunos routers en la ruta), y grabación de la ruta.

El nivel de transporte

El quinto nivel utiliza los servicios del nivel de red para proveer un servicio eficiente y confiable a sus clientes, que normalmente son los procesos en el nivel de aplicación. El hardware y software dentro del nivel de transporte se llaman la *entidad de transporte*. Puede estar en el corazón del sistema operativo, en un programa, en una tarjeta, etc. Sus servicios son muy semejantes a los del nivel de red. Las direcciones y el control de flujo son semejantes también.

Por lo tanto, ¿por qué tenemos un nivel de transporte? ¿Por qué no solamente el nivel de red? La razón es que el nivel de red es una parte de la subred y los usuarios no tienen ningún control sobre ella. El nivel de transporte permite que los usuarios puedan mejorar el servicio del nivel de red (que puede perder paquetes, puede tener routers que no funcionan a veces, etc.). El nivel de transporte permite que tengamos un servicio más confiable que el nivel de red. También, las funciones del nivel de transporte pueden ser independiente de las funciones del nivel de red. Las aplicaciones pueden usar estas funciones para funcionar en cualquier tipo de red.

Protocolos de transporte

Los protocolos de transporte se parecen los protocolos de enlace. Ambos manejan el control de errores, el control de flujo, la secuencia de paquetes, etc. Pero hay diferencias:

En el nivel de transporte, se necesita una manera para especificar la dirección del destino. En el nivel de enlace está solamente el enlace.

En el nivel de enlace es fácil establecer la conexión; el host en el otro extremo del enlace está siempre allí. En el nivel de transporte este proceso es mucho más difícil.

Establecimiento de una conexión

Desconexión

La desconexión asimétrica puede perder datos. La desconexión simétrica permite que cada lado pueda liberar una dirección de la conexión a la vez.

Control de flujo

Se debe controlar que el número de paquetes enviados a un destino para que no colapse a este.

Multiplexación

A veces el nivel de transporte tiene que multiplexar las conexiones. Si se desea una transmisión de datos muy rápida se abrirán varias conexiones y los datos se dividirán para hacerlos pasar por estas.

Si solo se tiene una conexión pero se quieren pasar varios datos se deberá multiplexar el canal. Por tiempos transmitirá una conexión u otra.

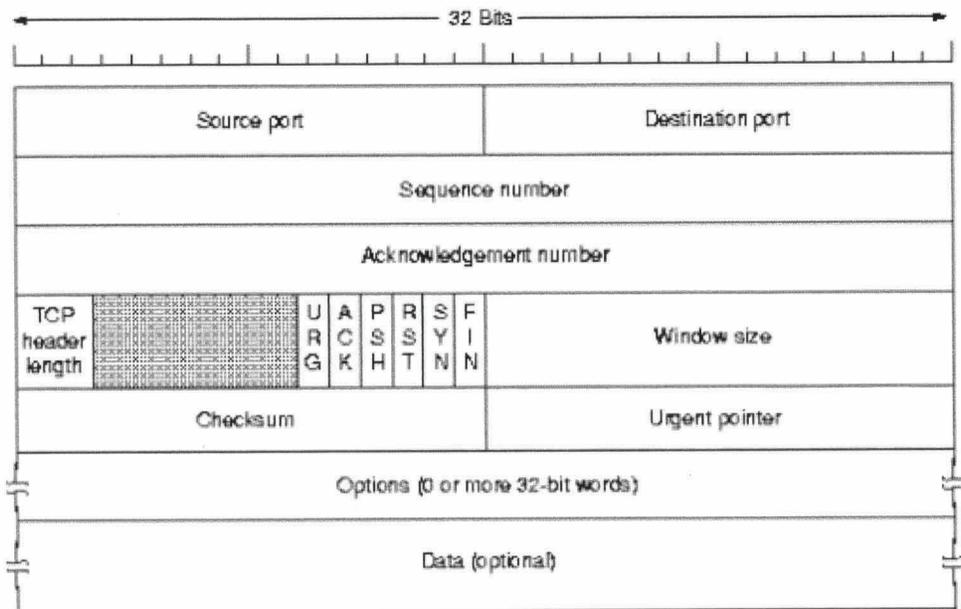
Recuperación de caídas

Si una parte de la subred se cae durante una conexión, el nivel de transporte puede establecer una conexión nueva y recuperar de la situación.

El encabezamiento de TCP

TCP (Protocolo de control de transmisión) es el método usado por el protocolo IP (Internet protocol) para enviar datos a través de la red. Mientras IP cuida del manejo del envío de los datos, TCP cuida el trato individual de cada uno de ellos (llamados comúnmente "paquetes") para el correcto enrutamiento de los mismos a través de Internet.

El encabezamiento de TCP para la transmisión de datos tienen este aspecto:



La puerta de la fuente y del destino identifica la conexión. El número de secuencia y el número de acuse de recibo son normales.

El último especifica el próximo byte esperado.

La longitud (4 bits) indica el número de palabras de 32 bits en el encabezamiento, ya que el campo de opciones tiene una longitud variable.

Los flags:

URG. Indica que el segmento contiene datos urgentes. El *puntero urgente* apunta al desplazamiento del número de secuencia corriente donde están los datos urgentes.

ACK. Indica que hay un número de acuse en el campo de acuse.

PSH (Push). El receptor no debiera almacenar los datos antes de entregarlos.

RST (Reset). Hay un problema en la conexión.

SYN. Se usa para establecer las conexiones. Una solicitud de conexión tiene SYN = 1 y ACK = 0, mientras que la aceptación de una conexión tiene SYN = 1 y ACK = 1.

FIN. Indica que el mandador no tiene más datos a mandar. La desconexión es simétrica.

TCP usa una ventana de tamaño variable. Este campo indica cuantos bytes se pueden mandar después del byte de acuse.

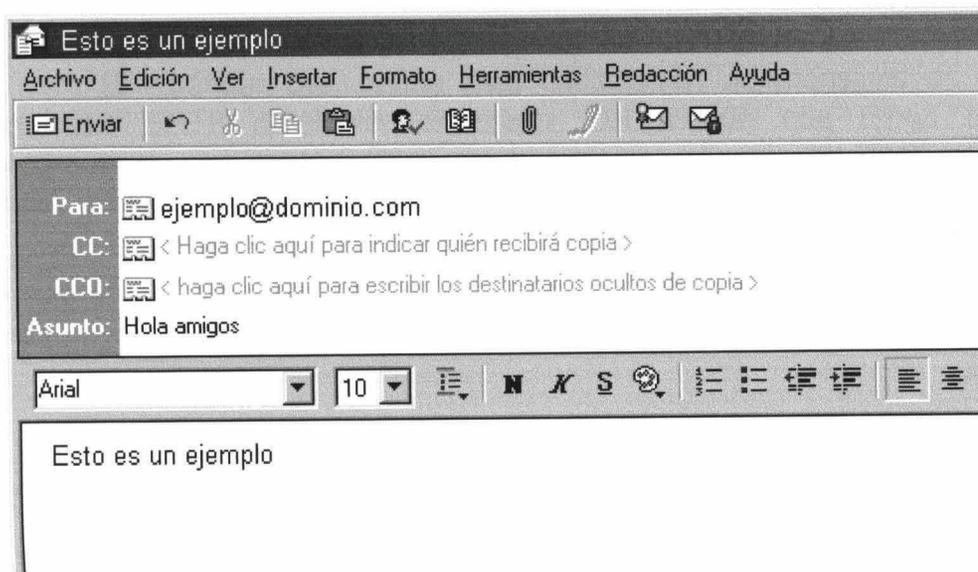
El checksum provee más confiabilidad. Las opciones permiten que los hosts puedan especificar el segmento máximo que están listos para aceptar (tienen que poder recibir segmentos de 556 bytes), usar una ventana mayor que 64K bytes, y usar repetir selectivamente en vez de repetir un número indeterminado de veces.

El nivel de aplicación

El nivel de aplicación es siempre el más cercano al usuario. Por nivel de aplicación se entiende el programa o conjunto de programas que generan una información para que esta viaje por la red. El ejemplo más inmediato sería el del correo electrónico.

Cuando procesamos y enviamos un correo electrónico este puede ir en principio a cualquier lugar del mundo, y ser leído en cualquier tipo de ordenador. Los juegos de caracteres utilizados por el emisor y el receptor pueden ser diferentes por lo que alguien se ha de ocupar de llevar a cabo estos ajustes. También se ha de crear un estándar en lo que la asignación de direcciones de correo se refiere. De todas estas funciones se encarga el nivel de aplicación. El nivel de aplicación mediante la definición de protocolos asegura una estandarización de las aplicaciones de red. En nuestro ejemplo del correo electrónico esto es lo que sucedería.....

Supongamos que escribimos un mensaje como el siguiente:



En nuestro caso hemos escrito este e-mail en un ordenador PC con Windows98 con el programa de correo Microsoft Outlook.

Fuese cual fuese el ordenador, sistema operativo o programa de correo que utilizásemos, lo que finalmente viajaría por la red cuando enviáramos el correo sería algo como esto:

```
From: " Remitente " E-mail del remitente
To: Destinatario
Subject: Hola amigos
Date: Thu, 25 Feb 2010 09:44:14 +0100
MIME-Version: 1.0
Content-Type: text/plain;
  charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3
```

Hola amigos

El estándar que define esta codificación de mensajes es el protocolo SMTP. Cualquier ordenador del mundo que tenga un programa de correo electrónico que cumpla con el estándar SMTP será capaz de sacar por pantalla nuestro mensaje.

5. - El cableado de la red.

El cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN. Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Estos son los tipos de cable más utilizados en redes LAN:

- Cable de par trenzado sin apantallar / UTP Unshielded twisted pair
- Cable de par trenzado apantallado / STP Shielded twisted pair
- Cable coaxial
- Cable de fibra óptica
- LAN 's sin cableado

5.1. - Cable de par trenzado sin apantallar / Unshielded Twisted Pair (UTP) Cable

Este tipo de cable es el más utilizado. Tiene una variante con apantallamiento pero la variante sin apantallamiento suele ser la mejor opción para una PYME.

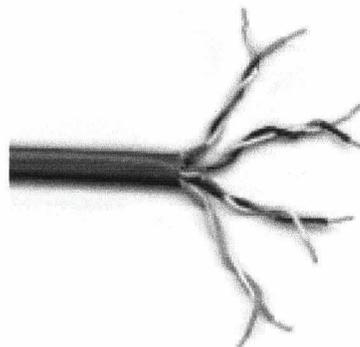


Fig.1. UTP

La calidad del cable y consecuentemente la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable. Las gradaciones van desde el cable de teléfono, que solo transmite la voz humana a el cable de categoría 5 capaz de transferir 100Megabytes por segundo.

5.1.1. - Categorías UTP

Tipo	Uso
Categoría1	Voz (Cable de teléfono)
Categoría 2	Datos a 4 Mbps (LocalTalk)
Categoría 3	Datos a10 Mbps (Ethernet)
Categoría 4	Datos a 20 Mbps/16 Mbps Token Ring
Categoría 5	Datos a 100 Mbps (Fast Ethernet)

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas).

Es conveniente sin embargo utilizar cables de categoría 5 ya que estos permitirán migraciones de tecnologías 10Mb a tecnología 100 Mb.

5.1.2. - Conector UTP

El estandar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. La siglas RJ se refieren al estandar Registerd Jack, creado por la industria telefónica.

Este estandar define la colocación de los cables en su pin correspondiente.



Fig.2. Conector RJ-45

5.2. - Cable de par trenzado pantallado / Shielded Twisted Pair (STP) Cable

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este problema existe un tipo de cable UTP que lleva apantallamiento, esto es, protección contra interferencias eléctricas. Este tipo de cable se utiliza con frecuencia en redes con topología Token Ring.

5.3. - Cable Coaxial

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.

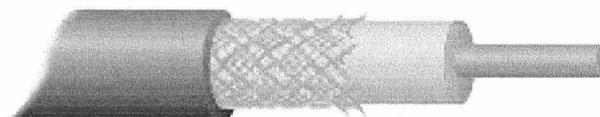


Fig.3. Cable Coaxial

Aunque la instalación del cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias. Por otra parte también es posible conectar distancias mayores que con los cables de par trenzado. Existen dos tipos de cable coaxial, el fino y el grueso conocidos como thin coaxial y thick coaxial.

Con frecuencia se pueden escuchar referencias al cable coaxial fino como thinnet o 10Base2. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial fino, donde el 2 significa que el mayor segmento posible es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología de BUS.

Con frecuencia se pueden escuchar referencias al cable coaxial grueso como thicknet o 10Base5. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial grueso, donde el 5 significa que el mayor segmento posible es de 500 metros. El cable coaxial es muy popular en las redes con topología de BUS.

El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace de este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar.

5.3.1. - Conector para cable coaxial

El más usado es el conector BNC. BNC son las siglas de Bayone-Neill-Concelman. Los conectores BNC pueden ser de tres tipos: normal, terminadores y conectores en T.

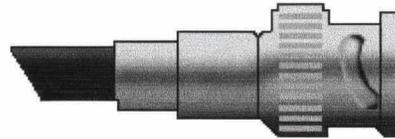


Fig.4. BNC connector

5.4. - Cable de fibra óptica

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar.

Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencia o servicios interactivos.

El coste es similar al cable coaxial o al cable UPT pero las dificultades de instalación y modificación son mayores. En algunas ocasiones escucharemos 10BaseF como referencia a este tipo de cableado. En realidad estas siglas hablan de una red Ethernet con cableado de fibra óptica.



Fig.5. Cable de fibra óptica

Características:

- El aislante exterior está hecho de teflón o PVC.
- Fibras Kevlar ayudan a dar fuerza al cable y hacer más difícil su ruptura.
- Se utiliza un recubrimiento de plástico para albergar a la fibra central.
- El centro del cable está hecho de cristal o de fibras plásticas.

5.4.1. - Conectores para fibra óptica

El conector de fibra óptica más utilizado es el conector ST. Tiene una apariencia similar a los conectores BNC. También se utilizan, cada vez con más frecuencia conectores SC, de uso más fácil.

5.5. - Resumen de tipos de cables empleados

Especificación	Tipo de Cable	Longitud Máxima
10BaseT	U T P	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fibra Optica	2000 meters

5.6. - Redes LAN sin cableado

No todas las redes se implementan sobre un cableado. Existen redes que utilizan señales de radio de alta frecuencia o haces infrarrojos para comunicarse. Cada punto de la red tiene una antena desde la que emite y recibe. Para largas distancias se pueden utilizar teléfonos móviles o satélites.

Este tipo de conexión está especialmente indicada para su uso con portátiles o para edificios viejos en los que es imposible instalar un cableado.

Las desventajas de este tipo de redes es sus altos costes, su susceptibilidad a las intereferencias electromagnéticas y la baja seguridad que ofrecen. Además son más lentas que las redes que utilizan cableado.

6. - PRINCIPALES TIPOS DE TOPOLOGÍAS FÍSICAS.

- Topología de Bus / Linear Bus
- Topología de Estrella / Star
- Topología de Estrella Cableada / Star-Wired Ring
- Topología de Arbol / Tree
- Resumen

6.1. - TOPOLOGÍA DE BUS / LINEAR BUS

Consiste en un cable con un terminador en cada extremo del que se "cuelgan" todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable. Este cable recibe el nombre de "Backbone Cable". Tanto Ethernet como LocalTalk pueden utilizar esta topología.

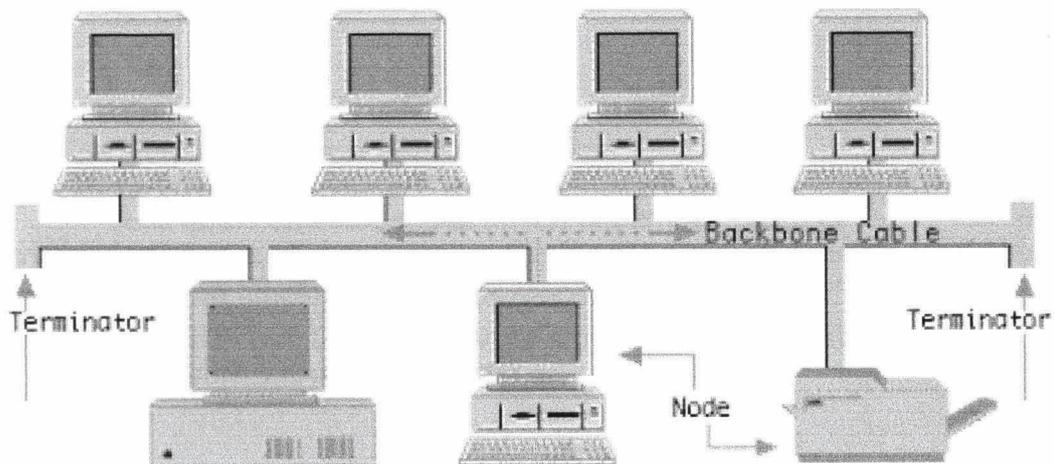


Fig. 1. Topología de Bus

6.1.1. - VENTAJAS DE LA TOPOLOGÍA DE BUS

- Es fácil conectar nuevos nodos a la red.
- Requiere menos cable que una topología estrella.

Desventajas de la topología de Bus

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requieren terminadores.
- Es difícil detectar el origen de un problema cuando toda la red "cae".
- No se debe utilizar como única solución en un gran edificio.

6.2. - TOPOLOGÍA DE ESTRELLA / STAR

En una topología estrella todos y cada uno de los nodos de la red se conectan a un concentrador o hub.

Los datos en estas redes fluyen del emisor hasta el concentrador. Este controla realiza todas las funciones de red además de actuar como amplificador de los datos. Esta configuración se suele utilizar con cables de par trenzado aunque también es posible llevarla a cabo con cable coaxial o fibra óptica.

Tanto Ethernet como LocalTalk utilizan este tipo de tipología.

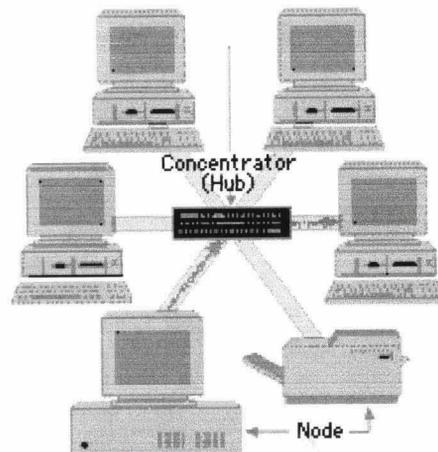


Fig.2. Tipología estrella

6.2.1. - VENTAJAS DE LA TOPOLOGÍA DE ESTRELLA

- Gran facilidad de instalación.
- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y su reparación.

Inconvenientes de la topología de estrella

- Requiere más cable que la topología de bus.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
- Se han de comprar hubs o concentradores.

6.3. - TOPOLOGÍA DE ESTRELLA CABLEADA / STAR-WIRED RING

Físicamente parece una topología estrella pero el tipo de concentrador utilizado, la MAU se encarga de interconectar internamente la red en forma de anillo.

Esta topología es la que se utiliza en redes Token-Ring.

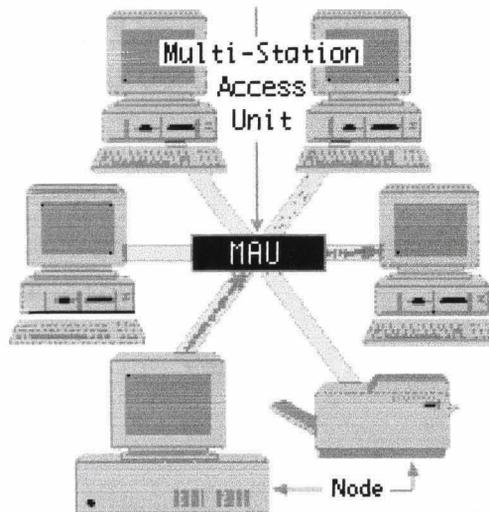


Fig.3. Topología de estrella cableada

6.4. - TOPOLOGÍA DE ARBOL / TREE

La topología de árbol combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red.

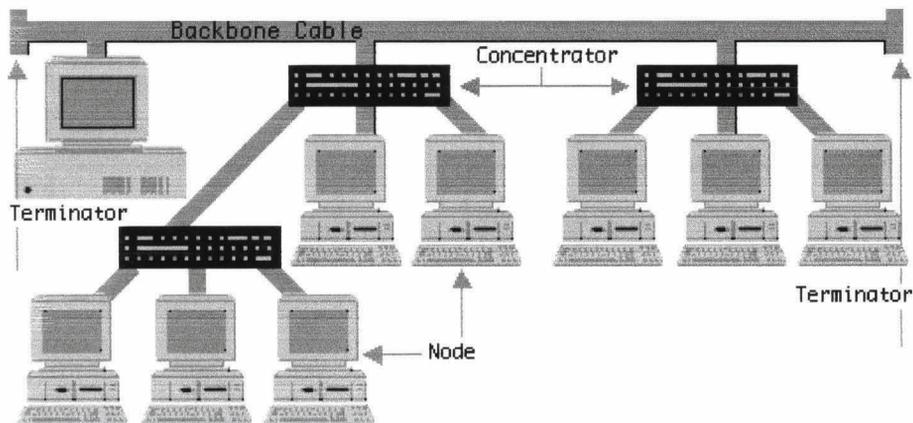


Fig.4. Topología de árbol.

6.4.1. - VENTAJAS DE LA TOPOLOGÍA DE ÁRBOL

- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Inconvenientes de la topología de árbol

- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo.
- Es más difícil la configuración.

Resumen :

Topología	Cableado	Protocolo
Bus	Coaxial Par Trenzado Fibra óptica	Ethernet LocalTalk
Estrella	Par trenzado Fibra óptica	Ethernet LocalTalk
Estrella en Anillo	Par trenzado	Token Ring
Arbol	Coaxial Par trenzado Fibra óptica	Ethernet

6.5. - PROTOCOLOS EN REDES LAN

Un protocolo es un conjunto de normas que rigen la comunicación entre las computadoras de una red. Estas normas especifican que tipo de cables se utilizarán, que topología tendrá la red, que velocidad tendrán las comunicaciones y de que forma se accederá al cana de transmisión.

Los estándares más populares son:

- Ethernet
- LocalTalk
- Token Ring
- FDDI

6.5.1. - ETHERNET

Ethernet es hoy en día el standard para la redes de área local. Tanto Ethernet (Versión 2) como el muy similar estándar IEEE802.3 definen un modo de acceso múltiple y de detección de colisiones, es el conocido *carrier sense multiple access/collision detection (CSMA/CD)*.

Cuando una estación quiere acceder a la red escucha si hay alguna transmisión en curso y si no es así transmite. En el caso de que dos redes detecten probabilidad de emitir y emitan al mismo tiempo se producirá una colisión pero esto queda resuelto con los sensores de colisión que detectan esto y fuerzan una retransmisión de la información.

Puedes ver un ejemplo de esto último pulsando en el siguiente esquema.

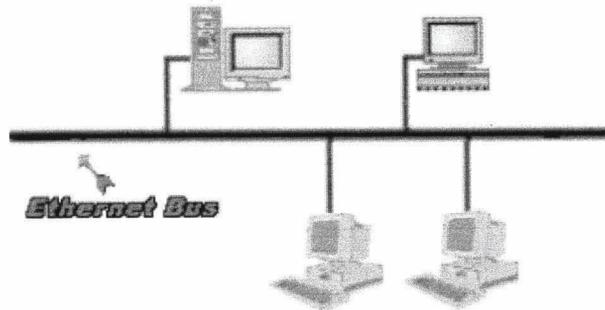


Ilustración de un bus Ethernet

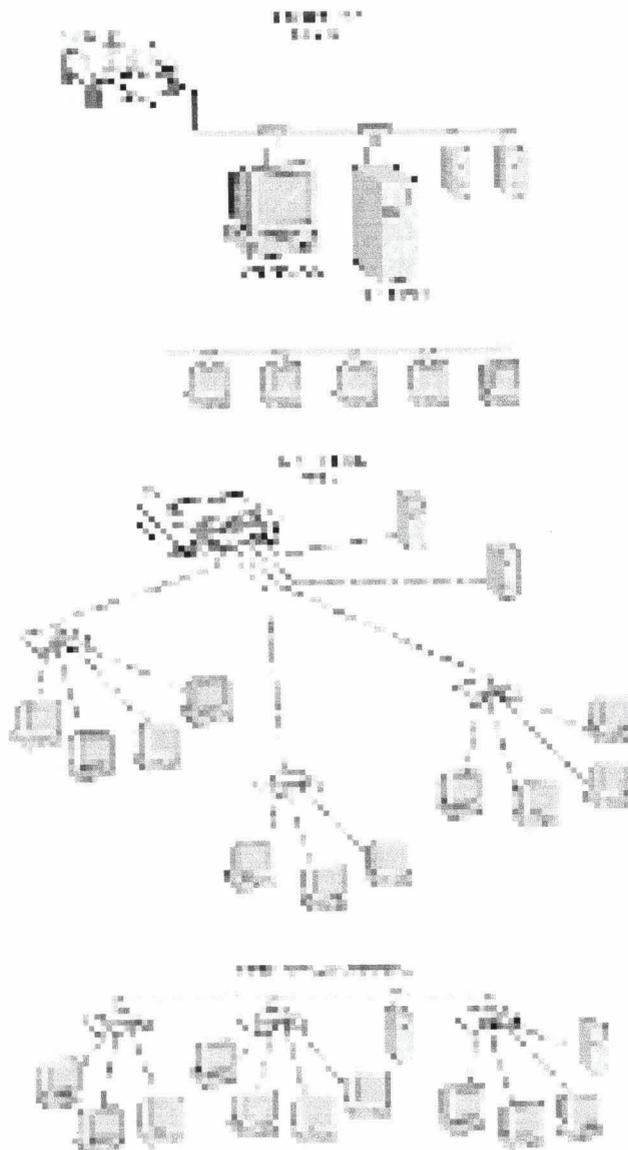
Cableados

- Velocidades de transmisión

Tipo de Ethernet	Velocidad (Mbps)	Distancia (m)	Media
10Base5 (IEEE 802.3)	10	500	Coaxial Grueso
10Base2 (IEEE 802.3)	10	185	Coaxial Fino
10BaseT (IEEE 802.3)	10	100	UTP
10BaseF(IEEE 802.3)	10	2000	Fibra Optica

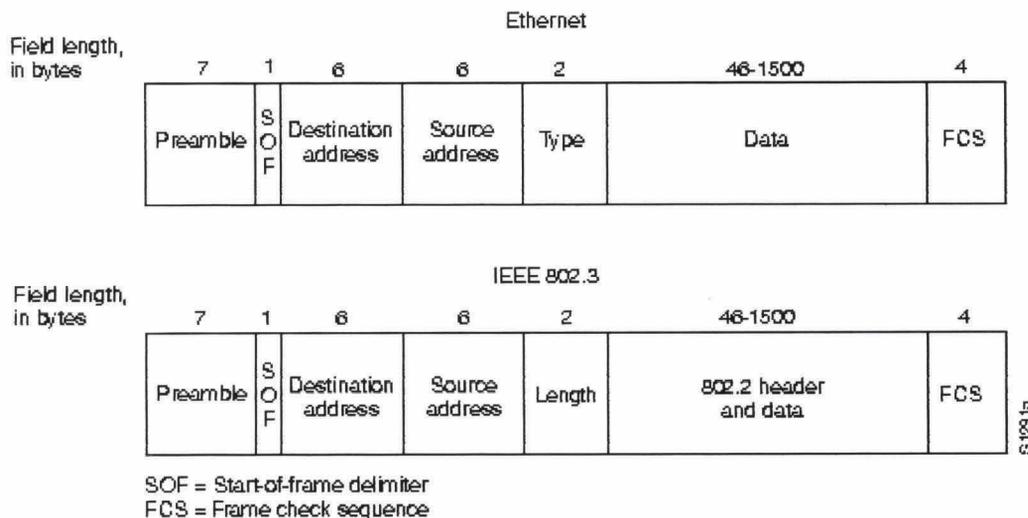
Topología

El protocolo Ethernet permite tres tipos de topología: Bus, Estrella y Arbol.(Linear Bus, star y Tree).



FORMATOS DE TRAMA

Formatos de trama Ethernet IEEE 802.3



Ethernet define de que manera se introducirán los datos en la red. Donde se indicará el receptor, el emisor donde irán los datos, donde irá el checksum, etc.. Esto se define en la trama Ethernet. En la figura superior se puede ver la distribución de las información en cada paquete enviado. Se comienza con un preámbulo que termina al que sigue la trama en sí. El inicio de la trama es la información de la dirección de destino seguido de la dirección de procedencia a lo que sigue el tipo o la longitud de la información los datos y el checksum de la trama. El checksum (FCS) se comprueba en la llegada para asegurarse de la correcta recepción de la información.

Fast Ethernet

Para aumentar la velocidad de la red de 10Mbps a 100Mbps se han definido nuevos estándares de Ethernet denominados en conjunto FastEthernet (IEEE802.3u). Tres nuevos tipos de redes Ethernet han visto la luz.

Las topologías posibles quedan reducidas a la topología estrella.

Tipo de Ethernet	Velocidad (Mbps)	Media
100BaseTX (IEEE 802.3u)	100	UTP de categoría 5
100BaseFX (IEEE 802.3u)	100	Fibra óptica
100BaseT4 (IEEE 802.3u)	100	UTP de categoría 3 modificado *

* Se añaden dos líneas al cable UTP de categoría 3.

6.5.2. - LOCALTALK

El protocolo LocalTalk fue desarrollado por Apple Computer, Inc. para ordenadores Macintosh. El método de acceso al medio es el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Este método, similar al de Ethernet (CSMA/CD) se diferencia en que el ordenador anuncia su transmisión antes de realizarla. Mediante el uso de adaptadores LocalTalk y cables UTP especiales se puede crear una red de ordenadores Mac a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional aunque se puede crear una red cliente servidor con el software AppleShare.

Con el protocolo LocalTalk se pueden utilizar topologías bus, estrella o árbol usando cable UTP pero la velocidad de transmisión es muy inferior a la de Ethernet.

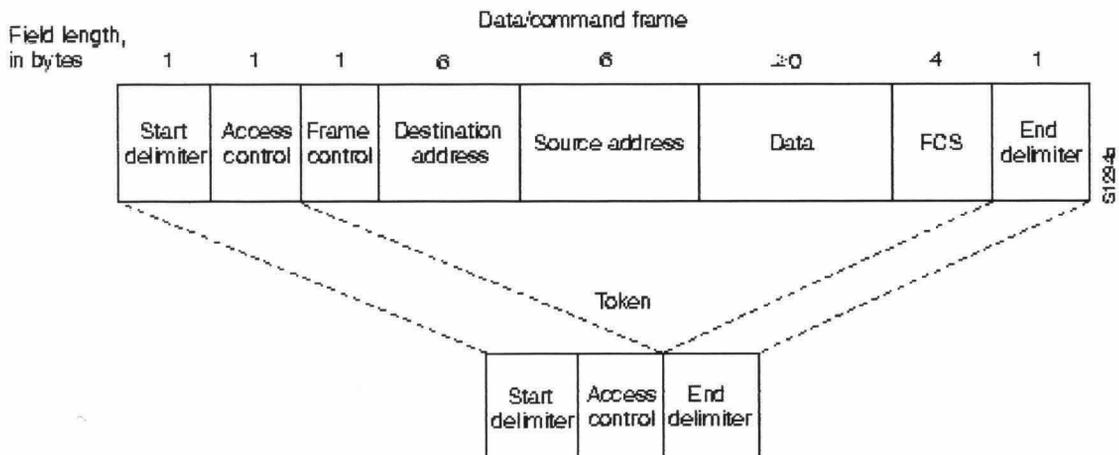
6.5.3. - TOKEN RING

El protocolo Token Ring fue desarrollado por IBM a mediados de los 80. El modo de acceso al medio esta basado en el traspaso del testigo (token passing). En una red Token Ring los ordenadores se conectan formando un anillo. Un testigo (token) electrónico pasa de un ordenador a otro.

Cuando se recibe este testigo se está en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre una tipología estrella cableada (star-wired) con par trenzado o fibra óptica. Se puede transmitir información a 4 o 16 Mbs. Cabe decir que el auge de Ethernet está causando un descenso cada vez mayor del uso de esta tecnología.

Formatos de Trama

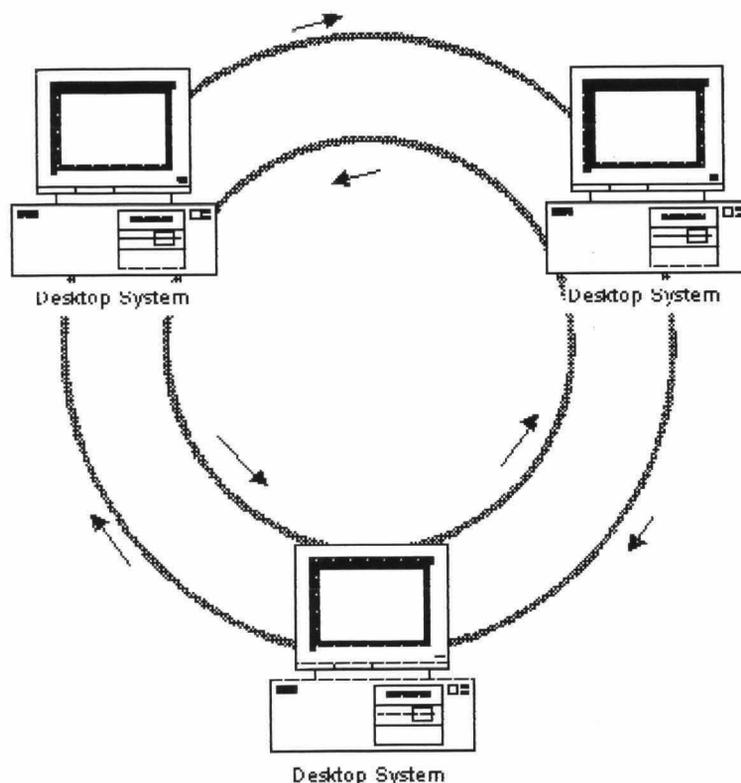
Tramas en Token Ring



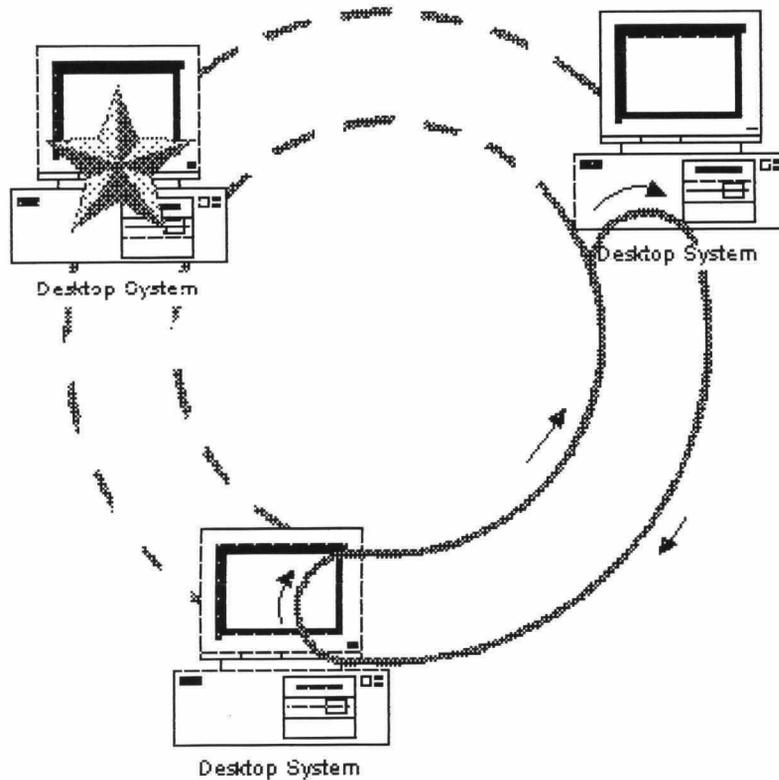
Como se puede ver, la trama de Token Ring es similar a la de Ethernet, la principal diferencia consiste en que a los datos se le agrega un Token, que es el que marca la prioridad de transmisi3n.

6.5.4. - FDDI

FDDI son las siglas de Fiber Distributed Data Interface . Este protocolo de red se utiliza principalmente para interconectar dos o m1s redes locales que con frecuencia distan grandes distancias.



El método de acceso al medio utilizado por FDDI está basado también en el paso de testigo. La diferencia es que en este tipo de redes la topología es de anillo dual. La transmisión se da en uno de los anillos pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión. Se monta sobre cables de fibra óptica y se pueden alcanzar velocidades de 100 Mbps.



6.6. - RESUMEN DE PROTOCOLOS

Protocolo	Cable	Velocidad	Topología
Ethernet	Par trenzado, coaxial, fibra óptica	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Par trenzado, fibra óptica	100 Mbps	Star
LocalTalk	Par trenzado	.23 Mbps	Linear Bus o Star
Token Ring	Par trenzado	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fibra óptica	100 Mbps	Anillo duall ring

7. - ETAPAS DE UNA RED LOCAL

Aspectos generales sobre la instalación de una red local.

Representar gráficamente toda la instalación. El instalador original del cableado telefónico existente podría ofrecernos documentación sobre éste. Anotaremos todos los problemas para futuras consultas.

Hablar con personas que hayan instalado sistemas similares de cableado de red, tales como miembros de un grupo local de usuarios de una red local.

Consultar la normativa sobre construcción correspondiente a nuestra zona y conocer los techos y paredes del edificio para evitar sorpresas. Podríamos encontrar muros de hormigón o placas antiincendios en lugares inesperados.

Debemos comprobar las placas de doble techo al buscar sitios para pasar el cable, y asegurarnos de evitar equipos eléctricos como acondicionadores de aire, cables de media tensión y fluorescentes.

Evitar extender el cable en pasillos y otras áreas de paso y asegurarse de que los puntos de conexión de estaciones están cerca de una toma de electricidad.

Planificar la instalación del cable y asignarle el tiempo suficiente para hacer bien el trabajo y trabajar fuera de horas de oficina cuando no se desee molestar a los empleados.

Al montar conectores de par trenzado, asegurarse de que los hilos se conectan a los terminales adecuados, al usar cable de par trenzado, comprobar la continuidad entre el cajetín telefónico y la estación de trabajo. Hay una serie de herramientas de verificación que se usan a tal efecto.

Si se utiliza cable coaxial, evitar doblar, arrugar, estirar o forzar el cable, ya que esto podría causar modificaciones en las características eléctricas del conductor y producir errores de transmisión de los paquetes.

Las bolas y piedras pueden ser las mejores amigas de un instalador. Atando una cuerda a una pelota de tenis, podremos tirársela a un colega para poder pasar un cable por un espacio cerrado. Una cuerda atada a una piedra puede bajarse por un orificio en la pared. Cuando se necesita introducir un cable por una instalación existente, pueden resultar útiles unas varillas finas de hilo de nylon resistente.

Los radioteléfonos son útiles cuando se necesita comunicarse con una persona que se encuentra al otro lado de una pared o techo, o a cierto número de pisos.

Evitar tender el cable cerca de luces fluorescentes en los dobles techos. Para evitar problemas, debemos planificar los tendidos con cable de sobra y también evitar pasar el cable cerca de otros cables eléctricos siempre que sea posible. Aunque el apantallamiento inhibe las interferencias, no está de más ser prevenido.

Fijar el cable con broches, grapas o abrazaderas y evitar doblarlo demasiado. No estirarlo al pasarlo por los conductores, asegurarse de que todos los tramos de cable son del mismo tipo y preferiblemente del mismo fabricante. El cable puede resultar parecido pero tener distintas características eléctricas. Un solo tramo de cable inadecuado puede causar problemas de transmisión en todo un segmento de la red.

La humedad puede deteriorar el cable, así que protegeremos los tendidos de cables externos de la acción de los elementos usando tubos u otras envolturas como canaletas.

Los tramos largos de cable son susceptibles a las interferencias. Los cables metálicos tienden a actuar como una antena que capta los campos eléctricos e interferencias de los dispositivos que encuentra a su paso.

A medida que se incrementa la longitud del cable, disminuye su capacidad de transmisión de señal. Si los programas de monitorización y análisis informan de un gran número de errores por reenvío de paquetes, esto podría señalar un problema de interferencias en el cable. Evitar problemas con las tomas a tierra.

Los problemas de cableado son relativamente fáciles de detectar en las redes configuradas en estrella. Si una estación no entra en comunicación con la red, verificaremos su tarjeta de red o el cable de conexión. Si fallan varias estaciones conectadas a un concentrador o hub, comprobaremos el concentrador.

7.1. - PRIMERA ETAPA DE UN LAN: DISEÑO

Planear cuidadosamente es la clave para una instalación exitosa. Existen actividades a las que mucha gente llama "más un arte que una ciencia", y aunque es una expresión un poco trillada, resulta bastante apropiada cuando se trata de diseñar una red.

Quizá no sea una disciplina artística, sino de una sabiduría casi instintiva que permite comprender la manera en que se mueve el tráfico en una red.

Casi todos los grandes fabricantes en el campo de redes, como Microsoft, y Cisco, tienen algún tipo de programa de certificación para diseño de redes, generalmente, suelen durar alrededor de una semana y son ampliamente recomendables para quienes comienzan a familiarizarse en este campo. Sin embargo, las horas de práctica ayudan a desarrollar un instinto para redes.

El proceso de diseño de una red está dividida en cuatro etapas:

- Determinar las necesidades.
- Diseñar la estructura de red (en papel).
- Realizar pruebas o elaborar un prototipo de la red.
- Instalar la red, paso por paso. Realizar el primer paso y evaluarlo; realizar el segundo paso y evaluarlo, y así sucesivamente.

Estos pasos son casi obvios cuando se reflexiona sobre ellos. Por desgracia, en el mundo real, la gran mayoría de redes se diseñan en el orden inverso. Primero se instala la red. Después someramente se estudia el diseño. Y finalmente se intenta definir qué hace falta para que la red funcione bien.

Determinar las necesidades puede ser el paso más difícil. Reemplazar una red ya existente, puede ser mucho más sencillo. Si no se cuenta con una red que pueda servir como base, lo que se debe saber es qué necesita la compañía que haga la red con exactitud. Seguramente habrá políticas de la empresa y discusiones territoriales. Aprender a convivir con ellas es normal.

Aunque no se pueda preguntar directamente, es necesario determinar las expectativas de los usuarios. Se determinará quiénes son los usuarios que requieren más recursos. Se debe tomar en cuenta que muchos usuarios que requieren recursos y conexiones de alta velocidad, con frecuencia no los necesitan en realidad. Por lo general, los usuarios que podrían obtener los beneficios de una conexión dedicada con gran ancho de banda ni siquiera están conscientes de ello.

Una vez que se cuenta con la lista de aplicaciones de redes que soportará la red, es momento de averiguar el ancho de banda requerido para cada aplicación. Se establecerá contacto con el fabricante o con los programadores que hayan desarrollado las aplicaciones, para saber cuál es el ancho de banda de red necesario para un número determinado de usuarios. Esta información servirá como punto de referencia. Asumir que los servicios centrales de redes requieren una conexión con gran ancho de banda, es un error común.

Por ejemplo, DHCP (Dynamic Host Configuration Protocol) y DNS (Domain Name Services) son absolutamente esenciales para una red basada en TCP/IP; por lo general, una red no funcionará sin ellos. Pero éstas son en realidad aplicaciones de bajo ancho de banda, así que las consideraciones de diseño para ellas deben estar basadas principalmente en la confiabilidad y en la tolerancia a fallas que en el ancho de banda de la red.

EL DISEÑO DE LA RED CON BASE A LA INFORMACIÓN ADQUIRIDA

Partiendo del caso de una red de gran eficiencia, asumiremos algún tipo de arquitectura con switches para la estructura de la red. Se determinará el ancho de banda necesario para soportar cada aplicación y para trabajar adecuadamente con el servidor.

Para aplicaciones de uso extremo, se podrán utilizar tarjetas 100BASE-T o incluso Gigabit Ethernet. Si se requiere más de 100-Mbps, pero sin llegar a velocidades de Gigabit, se considerará conectar dos tarjetas juntas para equilibrar las cargas de trabajo. La mayoría de los sistemas operativos y switches actuales ya lo soportan.

Por lo general, el mejor lugar para conectarse a un servidor es en la estructura principal o main backbone, lo cual por lo general le da a un servidor la mejor visibilidad posible. Pero si se sabe que la gran parte del tráfico será local, a un grupo específico de usuarios, se tomará en cuenta la posibilidad de colocar el servidor cerca del grupo al cual da servicio (por supuesto, nos referimos a una cercanía electrónica; no es necesario colocar el servidor físicamente en esa área).

El lugar donde esté colocado el servidor tendrá una influencia decisiva sobre su eficiencia. Mientras menos puntos de procesamiento deba atravesar un paquete, más rápido llegará a su destino. Los servidores no especializados deberán estar localizados en un lugar central con respecto al backbone. Los servidores diseñados para dar servicio a un grupo pequeño de usuarios, tales como al departamento de contabilidad, se localizan mejor en el mismo segmento de la red que los usuarios.

En este punto será necesario establecer el esquema y las políticas para nombres y direcciones, además de ser el mejor momento para documentar todas las políticas de red, tales como contraseñas y otras cuestiones de seguridad. Muchas personas dejan la documentación hasta el último momento, pero si se deja para el final, por lo general nunca sale bien, ni a tiempo. Se elaborará un prototipo de la red si es posible.

Ya hemos hablado sobre la dificultad de obtener los requerimientos precisos para aplicaciones de redes. Al elaborar primero un prototipo, antes de la instalación, es posible verificar las necesidades reales de los servidores de aplicaciones y evitar problemas posteriores.

Las instalaciones de redes por lo general se hacen contra reloj y con muy poco tiempo de sobra, por lo que resulta difícil evaluar todas las aplicaciones de manera adecuada.

Sin embargo, la experiencia nos enseña que el tiempo que se invierte evaluando una aplicación antes de instalarla por completo ahorra tiempo a largo plazo. Durante la evaluación del prototipo, es conveniente utilizar un analizador de paquetes que pueda reportar el uso del ancho de banda y los errores, así como decodificar paquetes.

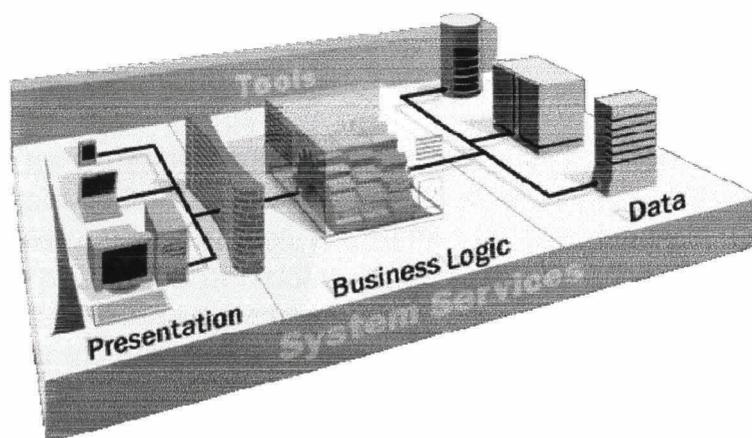
Este es el mejor momento para ajustar el diseño de red que se obtuvo en la segunda etapa. Con base en nuestra experiencia, es casi siempre necesario trabajar varias veces sobre el diseño de la red.

En el momento de la instalación de la red, se notará que enfatizamos el hecho de hacerlo paso por paso, deteniéndonos en cada punto para evaluar y verificar cada pieza de la red conforme se vaya instalando. Esto es porque resulta mucho más sencillo resolver problemas de la red cuando sólo existen un par de dispositivos, que podrían ser la causa del problema.

Con frecuencia se realizan instalaciones de toda la red y se trata de hacerla funcionar toda a la vez. Esa no es una buena idea, siempre habrá problemas con cualquier red nueva. Sin embargo, al instalar y probar pieza por pieza, mientras se verifica el proceso de instalación paso por paso, se simplifica la solución de los problemas. Se conservará la documentación actualizada y a la mano a lo largo de todo el proceso.

Incluso cosas aparentemente triviales como numerar las plaquetas de pared en cada oficina, puede resultar invaluable cuando surjan problemas más adelante. Siempre será mejor que sobre documentación y no que falte.

DIAGRAMACION DE UNA RED.



Antes de proceder a la instalación de una red, se la debe planificar. Si bien parece un paso obvio, muchas veces es saltado, con el resultado de que la red queda conformada por un conjunto de parches. Otro punto muy vinculado con éste, y también omitido, es el de documentar la instalación efectuada. Por empezar, la red debe tener como propósito por lo menos alguno de los siguientes (ya mencionados en este capítulo):

- Mantener bases de datos actualizadas instantáneamente y accesibles desde distintos puntos.
- Facilitar la transferencia de archivos entre miembros de un grupo de trabajo.
- Compartir periféricos caros (impresoras laser, plotters, discos ópticos, etc)
- Bajar el costo del software comprando licencias de uso múltiple en vez de muchas individuales.
- Mantener versiones actualizadas y coherentes del software.
- Facilitar la copia de respaldo de los datos.
- Correo electrónico.
- Comunicarse con otras redes (bridge).

Mantener usuarios remotos via modem.

Si las estaciones que forman la red poseen ROM de booteo pueden carecer de diskettera, con lo que además se logra:

- Evitar el uso ilegal del software.
- Evitar el ingreso de virus.
- Evitar el hurto de información.
- Facilita el acceso al sistema para usuarios inexpertos, ya que ingresa directamente a ejecutar sus aplicaciones.

LOS PASOS DE UN RED LOCAL EN BASE A OBJETIVOS:

En función de los objetivos elegidos los pasos a seguir son:

- 1) Determinar los usuarios y sus tareas. Esto incluye también el clasificar a los usuarios según aptitudes, nivel de seguridad en el que se desempeñarán y preveer si hay que capacitarlos. Cuestiones de seguridad y/o de baja capacitación pueden hacer recomendable el uso de estaciones sin disketteras y que arranquen desde el server.
- 2) Seleccionar los programas de aplicación a usar en cada estación. En este punto se elije la versión y cuántas licencias de uso hacen falta. Hay que asesorarse bien en cuanto al software ya que hay programas que tienen versiones especiales para red. Si se opta por programas multiusuario, aparte del descuento por licencia múltiple, ocupan menos lugar en el disco rígido.

3) También se decide dónde se los instala: algunos pueden ir en las estaciones, otros en el server. En general, conviene colocarlos todos en el server aunque haya algunos que sean usados por un sólo usuario, ya que le brinda la posibilidad de acceder al mismo desde otras estaciones.

Un caso muy frecuente es el de los puntos de venta. En estos casos conviene elegir programas que sean muy fáciles de usar, ya que el operador pasará casi todo el tiempo atendiendo al cliente.

Si se opta por un programa a medida, se lo deberá especificar y probar con sumo cuidado, tratando además que se pueda reconfigurar la mayor cantidad de cosas posibles sin intervención del programador. Siempre que se trabaje en redes, los costos e inconvenientes que implique una reprogramación se multiplican por la cantidad de puestos afectados.

Entre los programas a instalar, conviene tener un antivirus.

4) El programa de aplicación también define el sistema operativo que correrá en la estación.

5) En base a los requerimientos de software se dimensionan las estaciones de trabajo, ya que deben funcionar como soporte del programa. El dimensionado de las estaciones de trabajo incluye, entre otros tópicos:
tipo y velocidad del procesador.

cantidad y tipo de memoria (base, extendida, expandida).

Tipo de placa de video.

Si llevan disco rígido.

Si llevan diskettera (y de que formato).

6) En función de la cantidad de usuarios y de los servicios que deba brindar el sistema operativo de red se procede a seleccionar el mismo. Se debe considerar en este punto:

Si la red será basada en server o será entre pares.

Si el server correrá en modo dedicado o no.

Que para las grandes bases de datos conviene en casos extremos, se pueden usar servers duplicados. Otras posibilidades son el espejado y el "duplexing".

La futura expansión del sistema, ya que una versión para muchos más usuarios es innecesariamente cara, pero comprar "justo" y hacer "upgrades" periódicos puede ser más caro y ciertamente es más molesto.

7) Tal como ocurre con las estaciones, el sistema operativo a correr decide el hardware mínimo para el server. Debido a que en una red hay muchas más estaciones que servers, las estaciones se dimensionan "justas" mientras que el server se suele sobredimensionar. Al dimensionar el server se deciden: tipo y velocidad del procesador. (mínimo un CPU 600 mhz con 64Mb. de ram) cantidad de memoria (depende de la capacidad del disco rígido y otros componentes)

Tipo de placa de video. (no es relevante)

Cantidad y capacidad de los discos rígidos

Formato de la diskettera.

Necesidad de dispositivos tales como CD-ROM, unidades de cintas, etc.

Cantidad de puertas paralelo y serie.

8) Hay que decidir una estrategia de backup. En caso de decidirse por una cinta o un DAT, verificar que el software sea compatible con nuestro sistema operativo de red y ver en qué máquina se la ubica.

9) Hacer un plano con la distribución de máquinas, donde figuren las distancias entre ellas.

10) En función del tráfico estimado y de las distancias a cubrir, se decide el tipo de placas de red y el cableado. Esto implica: selección de la tecnología: Ethernet, Token ring u otras. Diagrama de cableado.

Si como consecuencia del tráfico o de violaciones de las distancias máximas conviene hacer puentes. En este caso se puede elegir entre uno interno o uno externo. tipo de bus al que se conectarán las placas de red: ISA de 8 o 16 bits, EISA, MCA o PCI.

Si se requiere una placa de red inteligente o con un gran buffer de comunicaciones. (especialmente en el server de una red con mucho tráfico). ROMs de "booteo remoto" para las estaciones que arranquen desde el server, con dispositivo de red WOL(wake on lan).

11) Determinar los equipos (como mínimo los servers, bridges y gateways) que tendrán fuente de alimentación ininterrumpible (UPS). Para ellos, se debe preveer si se usará algún sistema automático de detección de falta de electricidad (hay versiones con placa adaptadora y otros por puerta serie).

12) Aprovechando que se van a tender los cables de la red, es el momento de revisar la instalación eléctrica. En particular, es necesario asegurarse que los tomacorrientes tengan toma de tierra tanto para las computadoras como para los monitores e impresoras asociados. (Parece tonto, pero es muy importante, de esa manera evitaran "las patadas...")

13) Recién en este momento hacer la compra e instalación del hardware. Verificar el buen funcionamiento individual de las máquinas.

14) Documentar el hardware existente. Esto incluye tres aspectos: descripción completa de la configuración de cada máquina, que abarque no sólo los nombres de las placas sino también la posición de los jumpers y el setup del mainboard.

Plano de los cableados de la red, detallando los recorridos de los cables y las longitudes de los tramos afectados.

Documentación comercial asociada: vendedor, plazo de garantía, TE del servicio técnico, etc, de cada una de las partes. (Podría generarse una base de datos para facilitar esta tarea)

15) Proceder a instalar el software. Como se verá oportunamente, el sistema operativo de red pregunta datos sobre la controladora de disco y sobre la placa de red (direcciones, interrupciones, DMA, etc) por lo que conviene haber hecho a fondo la documentación que se sugiere en el punto 14.

16) Verificar que la red funcione, leyendo y escribiendo archivos desde las estaciones.

17) En base a los programas a instalar en el server y la lista de usuarios autorizados, se deberá diagramar el árbol de directorios y estudiar el tema de permisos y atributos de archivos. Es fundamental documentarlo correctamente y actualizarlo en forma periódica.

18) Instalar el software en el server, tomando en cuenta un antivirus robusto, y un firewall, por medida de seguridad.

19) Crear los usuarios y grupos, dotarlos de permisos, editar sus secuencias de conexión etc.

20) Prueba del sistema completo, así como la compartición de bases de datos, archivos, ficheros y dispositivos .

21) En los casos en los que se autorice a los usuarios a enviarse mensajes por la red, o que haya más de un server, se deberá dotar a los usuarios de una "guía" con los nombres de los usuarios y sus estaciones.

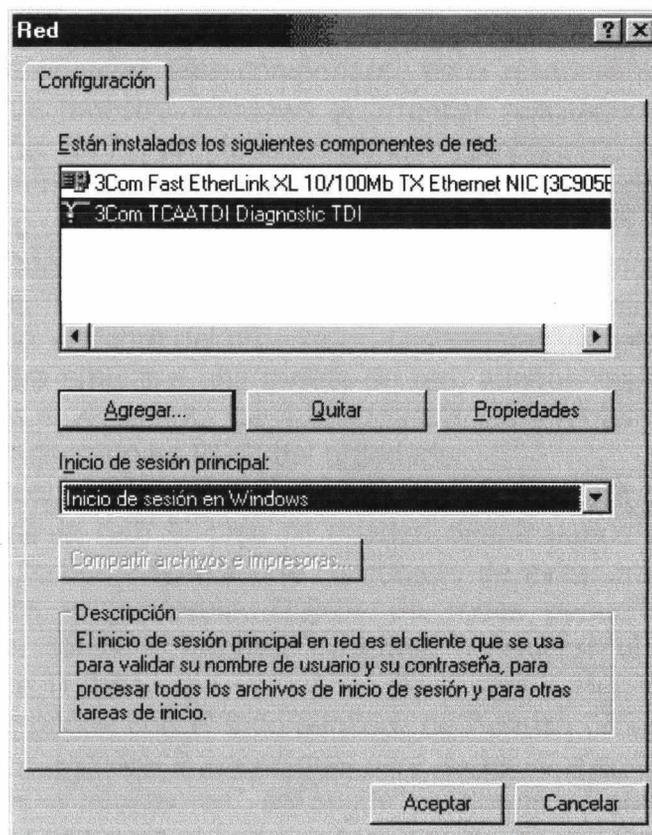
22) Administracion es la parte final de su planeacion, que es las actividades de administracion que deben realizarse en la red. Una valiosa herramienta para el desarrollo de una estrategia de administracion es establecer y mantener una bitacora del sistema. Esto es simplemente la documentacion bien guardada ya sea con una base de datos simple o con un sistema robusto que lleve el control de los usuarios, asi como las impresiones, archivos, actividades dentro de la red asi como correos electronicos e internet.

Nota: En junio de 2001 en un diplomado en "seguridad en redes" impartido a mas de 400 administradores de redes que asistimos, eramos un total de 18 personas los que utilizabamos algun tipo de bitacora menos de 5%, aun asi todos teniamos problemas con el manejo de nuestras redes.

8.- REDES LOCALES EN MS WINDOWS 95/98/MILLENIUM

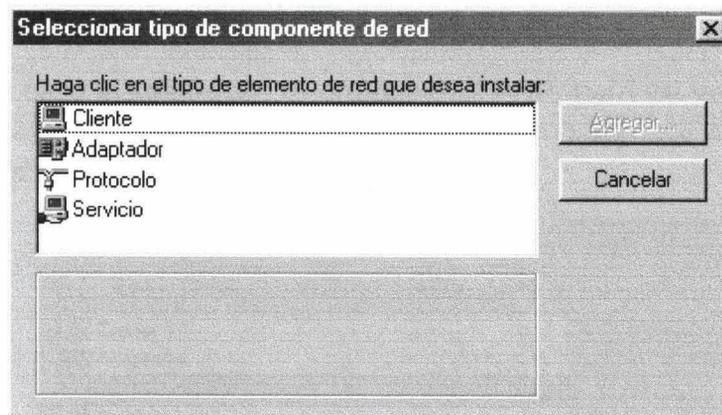
Para configurar nuestro sistema operativo de forma que podamos trabajar en red lo primero desde luego será comprar el cableado necesario e instalar la tarjeta de red. La tarjeta de red se instala como cualquier otra tarjeta que se instale en el ordenador. Si esta es Plug & Play (lo más habitual hoy en día), no tendremos más que pinchar la tarjeta, reiniciar el ordenador y seguir los pasos que nos indica el asistente. Si no es así deberemos instalar nosotros mismos la tarjeta a través del asistente "Agregar nuevo hardware" que se encuentra en el panel de control. Una vez instalada esta tarjeta ya podemos entrar en lo que es la auténtica configuración de red.

Para llevar a cabo cualquier configuración de red siempre hemos de seguir el mismo camino. Configuración, Panel de Control, Red. Con esto se despliega el siguiente cuadro.



Vemos que aparece la tarjeta de red y debajo un icono con la leyenda "3Com TCAATDI Diagnostic TDI", esto es lo que aparece cuando se instala la tarjeta de red, es decir, todo esto llega aquí automáticamente. ¿Qué es lo que hemos de añadir nosotros?

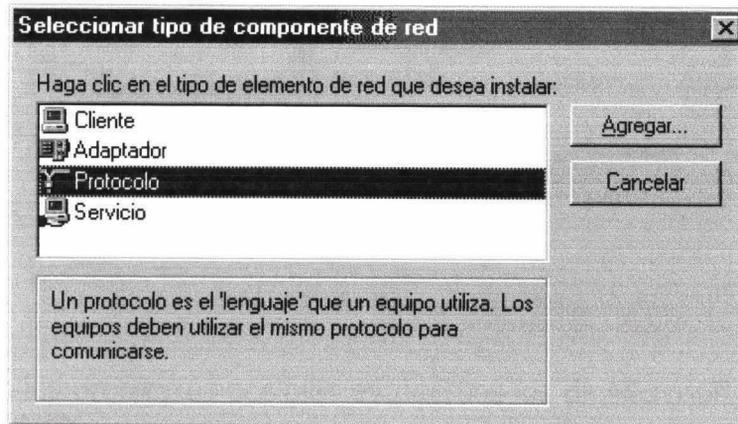
En propiedades de Entorno de red se definen **4 familias de componentes**:



1. **Cliente.** Permite acceder a recursos de otros puestos de la red. Utilizaremos el *Cliente para redes Microsoft*. Este componente es el responsable de la pantalla de Inicio de sesión que muestra Windows al arrancar solicitándonos un nombre de usuario y contraseña. En las propiedades de este componente se indica si estamos montando una red entre iguales (casilla "Iniciar sesión en el dominio de Windows NT" deshabilitada) o una red cliente/servidor (casilla habilitada).
2. **Adaptador.** Es cada tarjeta de red real o virtual que tengamos instalada en nuestro ordenador. Las tarjetas de red reales son aquellas que instalamos físicamente en algún *slot* libre del ordenador. Las tarjetas virtuales son aquellas que instala Windows para emular a una tarjeta de red, aunque realmente no exista. El caso más común es el *Adaptador de Acceso telefónico a redes* que se corresponde con los módems o adaptadores RDSI del ordenador.
3. **Protocolo.** Es el lenguaje que utiliza nuestro ordenador para comunicarse con el resto de puestos de la red. Si bien se pueden definir varios protocolos para un mismo adaptador, no es recomendable con objeto de evitar tráfico innecesario en la red. Utilizaremos el *protocolo TCP/IP*. En redes pequeñas (menos de 10 ordenadores) y sin salida a Internet podemos considerar el uso del protocolo NetBEUI en lugar de TCP/IP.
4. **Servicio.** Se corresponde con el lado servidor de nuestro ordenador. Utilizaremos el servicio *Compartir archivos e impresoras para redes Microsoft*. Mediante el botón "Compartir archivos e impresoras" se puede configurar si ofreceremos archivos, impresoras o ambos recursos al resto de equipos de la red. Este servicio necesita que esté instalado el *Cliente para redes Microsoft*.

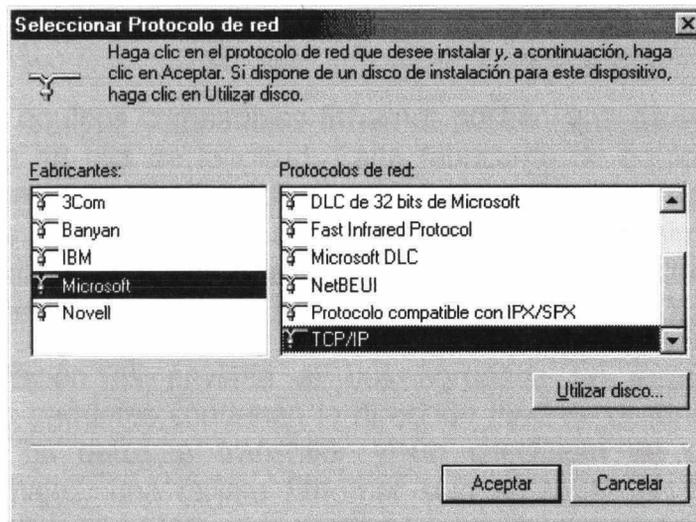
Para trabajar en red necesitamos en primer lugar una conexión física, como vemos esto ya está aquí por lo tanto el siguiente paso es la instalación de los protocolos.

En este caso instalaremos el protocolo TCP/IP, para así ver su configuración, de todas formas, la instalación de otro protocolo sería idéntica a esta. Para instalar un protocolo hemos de pulsar el botón "Agregar".



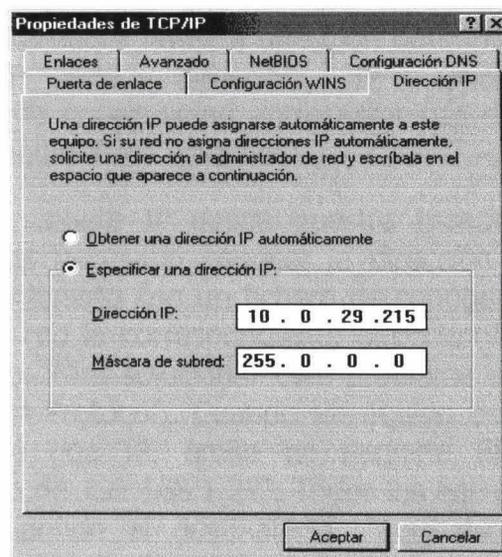
Aparecen cuatro opciones, agregar un cliente, agregar un Adaptador, agregar un Protocolo o agregar un Servicio. Agregar un adaptador instala una nueva tarjeta de red, agregar un protocolo instala un protocolo, lo mismo para servicio. Si agregamos un cliente se instalarán una serie de funciones que el sistema operativo necesita como funciones para trabajar con servidores Novell, o funciones para trabajar con servidores NT, es decir, se instalarán las funciones adicionales que el sistema operativo necesita para trabajar con otros servidores. Hay que decir que un cliente siempre necesitará que existan protocolos instalados, por ejemplo, el cliente para trabajar con servidores Novell exige que se haya instalado el protocolo IPX/SPX, de todas formas Windows se encargará de instalar automáticamente todos los protocolos necesarios por lo que no debemos preocuparnos por esto. Lo mismo ocurre con los servicios, los servicios son porciones del sistema operativo que permiten al ordenador llevar a cabo funciones de red como compartir archivos, impresoras, etc... Si un servicio requiere protocolos determinados ya instalados el sistema se encargará de instalarlos automáticamente.

En este caso vamos a construir la casa desde los cimientos, una vez instalada la tarjeta instalaremos el protocolo TCP/IP.



De todos los protocolos posibles escogemos los de Microsoft, y dentro de los de Microsoft TCP/IP.

Como podemos ver, aparte de TCP/IP ha aparecido el Cliente para redes Microsoft. Esto es porque Windows entiende que si estamos instalando TCP/IP es por que vamos a trabajar en red y para ello se necesitan ciertos añadidos sobre el sistema operativo, así que automáticamente se instala el Cliente para redes Microsoft. Más adelante habrá que configurar este cliente para redes. De momento configuraremos el protocolo instalado. Simplemente tenemos que señalar este protocolo y hacer clic en "Propiedades".



Métodos de comunicación

Direcciones MAC

Todos los equipos compatibles Ethernet poseen una **dirección MAC** única en el mundo, de 48 bits de longitud. Cada fabricante de equipos Ethernet tiene asignado un **segmento de direcciones**, y es responsabilidad de este asignar una **dirección distinta a cada equipo**. Las direcciones MAC están almacenadas en una pequeña memoria que poseen las tarjetas de red. Las direcciones MAC se representan en hexadecimal con el siguiente formato: **XX:XX:XX:XX:XX:XX**.

La información es enviada al bus agrupada en forma de **tramas o paquetes**. Estos paquetes contienen la dirección MAC de destino, la de origen, el tipo de datos, los datos a transmitir y un checksum de comprobación. En condiciones normales, una tarjeta Ethernet solo es capaz de "oír" los paquetes destinados a su dirección MAC o los destinados a todo el mundo (BROADCAST). La dirección MAC de BROADCAST es FF:FF:FF:FF:FF:FF

Protocolo IP Y ARP

El protocolo IP (Internet Protocol), es un protocolo de red con direcciones de 32 bits, bajo el conocido formato aaa.bbb.ccc.ddd, formando 4 grupos de 8 bits. La dirección de red IP puede ser dividida en dos partes, la dirección de red y la dirección de equipo. Si estamos en una red conectada a Internet, nuestra dirección de red será única en Internet, y nuestra dirección de equipo será única en nuestra red, formando así una dirección IP única a nivel global. Vamos a centrarnos en la conectividad entre máquinas de nuestra propia red IP, funcionando sobre un medio físico Ethernet.

Para enviar un paquete IP desde nuestra estación 192.168.1.1 hacia la estación 192.168.1.2, es necesario conocer la dirección MAC de la estación de destino. Podríamos solucionarlo con un fichero de configuración, asignando a cada dirección IP de nuestra red la correspondiente dirección MAC asociada a cada IP, pero sería poco práctico. Para solucionar este problema se desarrolló el protocolo ARP (Address Resolution Protocol). Cuando un equipo desea conocer la dirección MAC correspondiente a una IP, emite un paquete BROADCAST preguntando "¿Quién es el propietario de 192.168.1.2?". Todos los equipos de la red escuchan la petición, pero solo responde el destinatario: "aquí está 192.168.1.2 desde la dirección MAC xx:xx:xx:xx:xx". Esta respuesta se almacena en el caché ARP del peticionario para usos posteriores, y procede a enviar el paquete al destinatario

Configuración

A no ser que estemos en una red en la que haya un servidor (puede ser Unix, NT, linux, etc...) que se encargue de asignar **direcciones IP** automáticamente, a todos los equipos hemos de dar nosotros una dirección IP. Aparte de esto tendremos que asignar también una máscara de red. La dirección IP son cuatro dígitos separados por puntos al igual que la máscara de red. De estos cuatro números unos indican el número de red y otros el número de equipo dentro de la red. Qué dígitos son la red y cuales son el equipo. Depende de la máscara de red. Lo que hay "encima" del 255 es número de red y lo que hay encima del "0" es el número de equipo. En nuestro caso el estamos en la red 10 y somos el equipo 0.29.215. ¿Qué números utilizar para la máscara y para la dirección IP? Para la dirección IP se pueden utilizar número entre 0 y 255. Para la máscara veamos..... Los pares dirección Máscara de subred pueden ser de tres tipos

Tipo A:

Dirección IP: **1-126. 0-255. 0-255. 0-255**

Máscara de subred: **255. 0. 0. 0**

Tipo B:

Dirección IP: **128-191. 0-255. 0-255. 0-255**

Máscara de subred: **255. 255. 0 . 0**

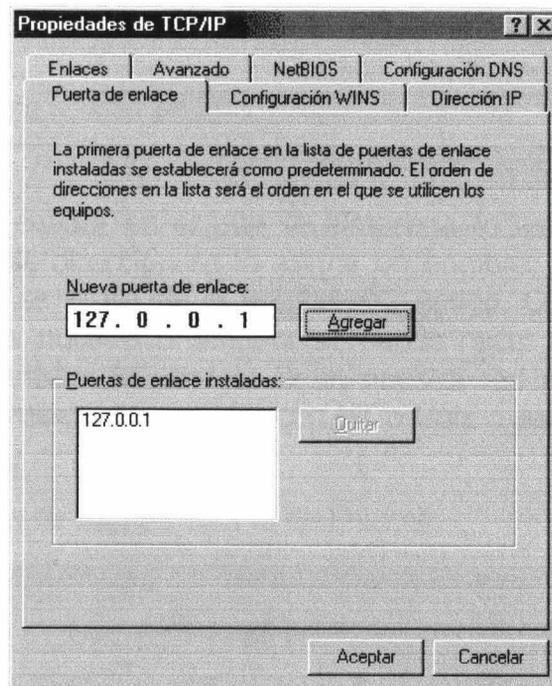
Tipo C:

Dirección IP: **192-223 . 0-255 . 0-255 . 0-255**

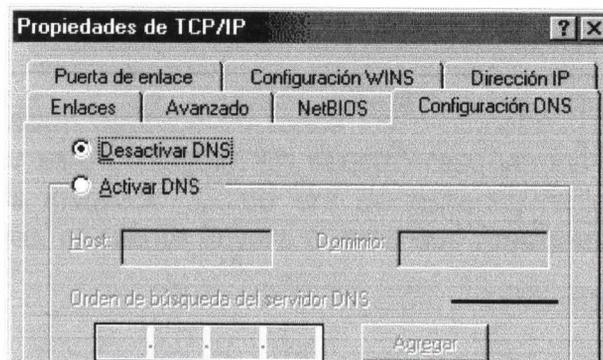
Máscara de subred: **255 . 255.255 . 0**

Para redes internas se utilizan direcciones Tipo A con el primer dígito (el de red) un 10. Así pues, pondremos una dirección como la de arriba. Con esto ya hemos configurado la parte más importante del protocolo TCP/IP.

Veamos ahora la configuración de la Pasarela o Puerta de enlace:



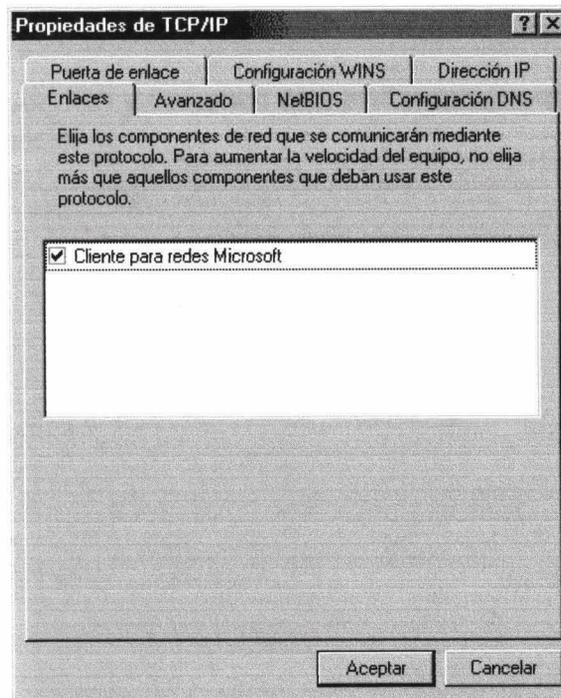
Según lo visto anteriormente, una dirección IP hace referencia a una red y a un equipo dentro de la red. En nuestro caso estamos en la red 10 y somos el equipo 0.29.25. Si quisiéramos conectar con un equipo de la red 11 deberíamos hacerlo a través de una puerta de enlace, esto es, un equipo que está en la red 10 y en la red 11 al mismo tiempo (esto se consigue con un servidor NT o Unix con dos tarjetas de red, cada una con una dirección). Aquí diremos quien es ese equipo. Si no existen dos redes el concepto de gateway no tiene sentido por lo que este campo se puede dejar en blanco o se puede poner la dirección que arriba vemos. Esta dirección en lenguaje TCP/IP significa el propio ordenador, es decir en este caso sería lo mismo poner 127.0.0.1 que 10.0.29.215.



Configuración DNS.

DNS es un ordenador en el que se almacena todas las direcciones de los equipos de red. A cada dirección se le asigna un nombre, por ejemplo a nuestra dirección 10.0.29.215 se le asigna el nombre PC_Amigo. Cualquier llamada futura que se quiera hacer a nuestro ordenador se puede hacer llamando al ordenador 10.0.29.215 o al ordenador PC_Amigo. Si en nuestra red no existe uno de estos ordenadores (habitualmente un servidor con NT o Unix o parecido) desactivaremos esta opción.

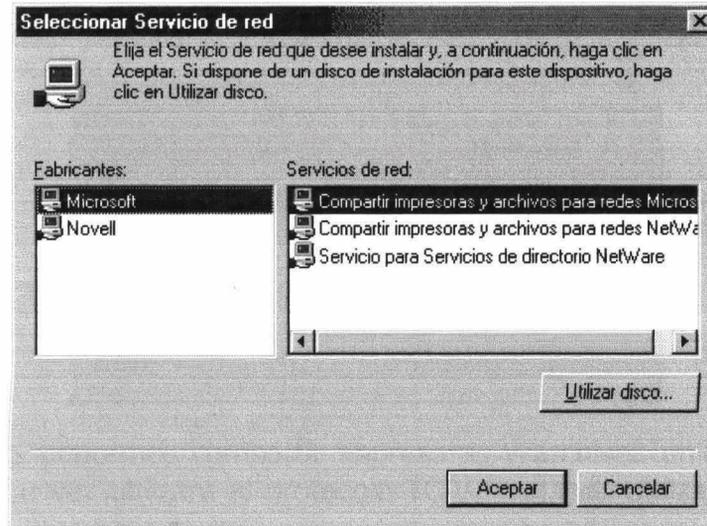
La última configuración de interés será la de Enlaces.



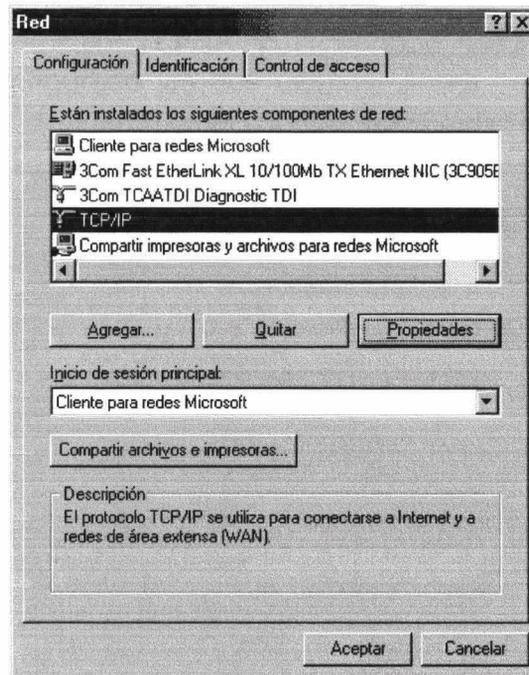
Esta configuración aparece en todos los protocolos. Indica que servicios o clientes van a utilizar este protocolo. En nuestro caso vemos que aparece el único cliente que tenemos instalado. Como era de esperar, teniendo únicamente un protocolo y un cliente, el cliente llevará a cabo sus funciones mediante el uso de este protocolo.

En caso de tener otros protocolos instalados podríamos decidir si un cliente va a utilizar este protocolo o va a utilizar otro, y los mismos para los servicios.

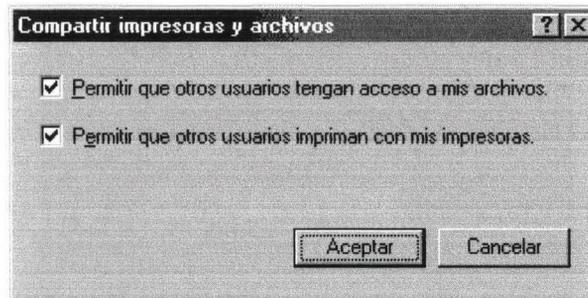
Una vez tenemos instalado el protocolo vamos a añadir un servicio que es la compartición de archivos e impresoras entre ordenadores. Para añadirlo elegimos añadir servicio...



Elegimos este servicio y veremos que en la pantalla de configuración de red aparece un nuevo servicio.



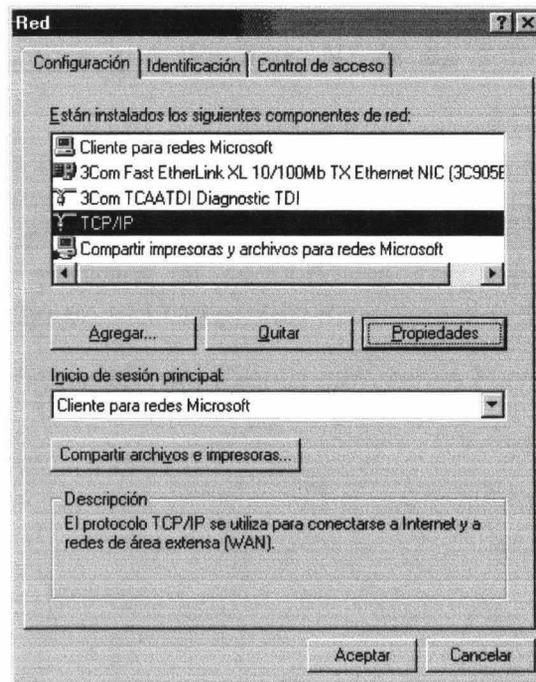
Un nuevo servicio llamado compartir impresoras y archivos para redes Microsoft ha aparecido. Si ahora hacemos doble click en Compartir archivos e impresoras podremos decidir si vamos a compartir archivos, impresoras, ambos o ninguno.



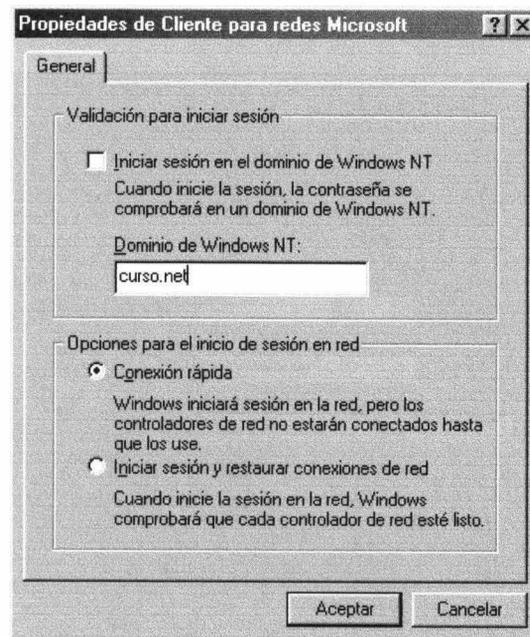
A partir de ahora podremos compartir impresoras y archivos utilizando el servicio instalado que a su vez utilizará al protocolo TCP/IP, el cual utilizará a la tarjeta de red instalada.

Ciente para redes Microsoft

Seguimos con la configuración de la red. Ya hemos instalado la tarjeta, hemos añadido el protocolo TCP/IP y el servicio para compartir archivos e impresoras. Hemos configurado los dos últimos. Ahora configuraremos el Cliente para redes Microsoft y terminaremos la configuración general de red.



Seleccionaremos Cliente para redes Microsoft y pulsaremos "Propiedades". Esto es lo que vemos:



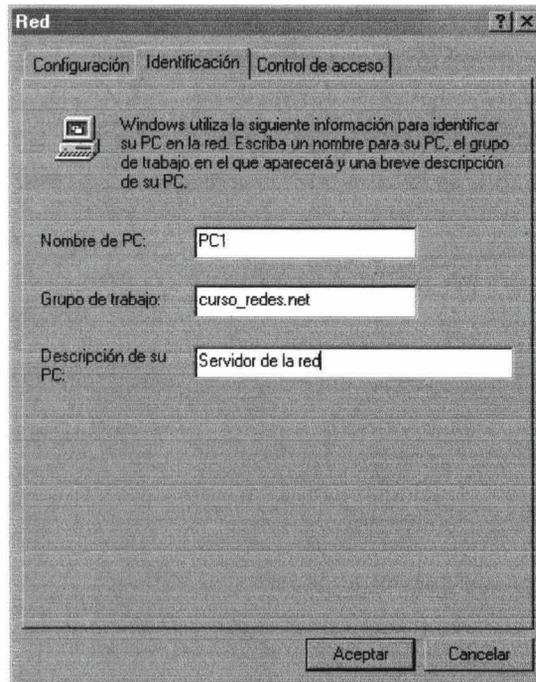
La primera opción que tenemos es iniciar una sesión en el dominio de Windows NT. Si en nuestra red existe un servidor NT y utilizamos recursos de este deberemos activar esa opción para que el servidor nos reconozca como usuarios y nos ofrezca sus servicios. Si la activamos nos pedirá un nombre de dominio, esto no es más que el nombre que Windows NT le da a la red, en nuestro caso curso.net.

Otra opción que aparece es la conexión rápida o el Inicio de sesión y la restauración de conexiones, si elegimos el primero no se cargarán en memoria los elementos necesarios para trabajar en red hasta que el usuario realice una operación de red, si elegimos el segundo se cargarán todos los elementos necesarios para el trabajo en red tan pronto iniciemos el ordenador.

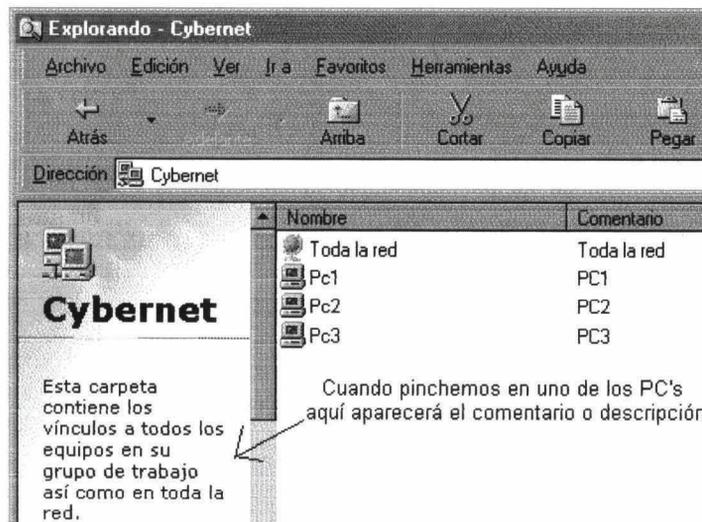
Con esto finaliza la configuración del Cliente para redes Microsoft.

GRUPOS DE TRABAJO

El siguiente paso es acabar con la configuración general de red. Para ello en propiedades de red deberemos señalar la pestaña de Identificación.

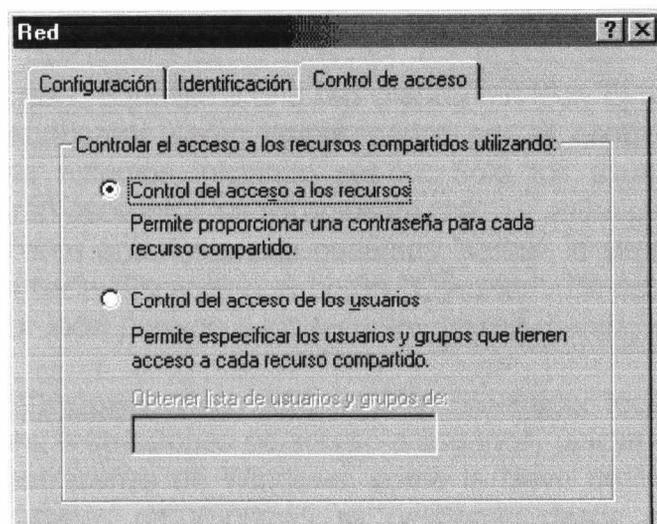


En esta ventana daremos un nombre a nuestro PC, podemos poner el que queramos. Este será el nombre con el que se verá a nuestro equipo en la red más adelante. También podemos introducir un comentario, este comentario será el que aparezca en la ventana de entorno de red cuando seleccionemos nuestro PC.



Un concepto importante que también aparece es el de grupo de trabajo. En capitulo mas adelante veremos que Windows NT y 2000 daba un nombre a la red, y ese nombre es conocido como el dominio. En caso de que no tengamos más que una red punto a punto el concepto de dominio desaparece pues no tenemos servidores NT, sin embargo, y siguiendo la misma filosofía el conjunto de la red recibe un nombre que es el de Grupo de trabajo. Todos los ordenadores de nuestra red deben permanecer al mismo grupo de trabajo o no será posible localizarlos mediante la ventana de entorno de red. En nuestro ejemplo los tres ordenadores que tenemos están en el grupo de trabajo curso_redes.net. Podría haber más ordenadores en la misma red (conectados físicamente) pero si no especificamos en la configuración de red de estos ordenadores que el grupo de trabajo al que están adscritos es curso_redes.net no nos podremos comunicar con ellos.

Con esto solo nos queda configurar el Control de Acceso para acabar con la configuración de red general.



Estamos en el último paso. Si decidimos compartir ficheros o impresoras de nuestro ordenador podemos especificar una contraseña para cada elemento compartido. Esta sería la primera opción. Sin embargo, si estamos en una red con un servidor NT, este tendrá una lista de todos los usuarios existentes y los permisos de uso que estos usuarios tienen en la red. Activando la segunda opción podemos utilizar la lista del servidor NT, solo habrá que especificar cual es el dominio de dicho servidor.

Contraseña de red Microsoft y contraseña de Windows

Windows utiliza dos tipos de contraseñas al iniciar sesión:

Contraseña de red Microsoft. Es necesaria para tener acceso a los recursos de la red. Nos valida como clientes de la red. Según hayamos configurado la casilla "Iniciar sesión en el dominio de Windows NT" de las propiedades de "Cliente para redes Microsoft" se dan los siguientes casos:

a. **Casilla desmarcada.** Equivale a una red entre iguales. Podemos escribir cualquier nombre de usuario / contraseña. Como no hay ningún ordenador que valide esta contraseña todas las que se nos ocurran serán válidas. No hay ninguna seguridad: cualquier usuario puede acceder a los recursos en red.

b. **Casilla marcada.** Equivale a una red cliente/servidor. El nombre de usuario / contraseña que escribamos serán comprobados por el controlador principal del dominio en el que estemos iniciando sesión. Sólo los usuarios correctamente autenticados podrán acceder a los recursos en red.

Nota: En los dos casos anteriores nos podemos "saltar" la ventana de contraseña de red pulsando la tecla "Escape" o el botón "Cancelar". De esta forma tendremos acceso al ordenador local pero no a los recursos en red.

Contraseña de Windows. Hace referencia al ordenador local, no a la red. Sin embargo, no impone restricciones de acceso a usuarios, únicamente es la llave que almacena otras contraseñas de Windows, como la clave de "Acceso telefónico a redes". Las contraseñas de Windows se gestionan desde Panel de control / Contraseñas. Solamente se le solicitará al usuario si la contraseña de red Microsoft que había tecleado anteriormente no coincide con una contraseña de Windows válida. Lo habitual, por tanto, es que ambas contraseñas coincidan para que el usuario sólo tenga que teclearla una vez.

Los usuarios que hayan iniciado sesión en un ordenador con una determinada contraseña deberán introducir la misma las siguientes veces. De lo contrario, el sistema no le permitirá el paso. Sin embargo, se puede dar de alta un nuevo usuario con sólo teclearlo.

Nota: Nos podemos "saltar" la ventana de contraseña de Windows pulsando la tecla "Escape" o el botón "Cancelar". Sin embargo, no nos aparecerá ninguna contraseña guardada en los cuadros de diálogo de Windows (tendremos que teclearlas nuevamente). Además, ciertos programas no serán capaces de almacenar nuestras preferencias personales.

Nota: Las contraseñas de Windows se almacenan en archivos *.pwl para cada usuario. Podemos eliminar todas las listas de contraseñas de Windows simplemente eliminando los archivos *.pwl almacenados en el directorio de Windows.

¿Cómo proceder? Lo habitual es escribir únicamente la contraseña de red Microsoft de forma que ésta coincida con la contraseña de Windows. La primera vez se nos solicitará confirmar la contraseña de Windows (el sistema estará creando un nuevo usuario), pero las siguientes veces únicamente tendremos que teclear la contraseña una sola vez (Windows advertirá que ambas contraseñas coinciden). Según las explicaciones anteriores, debemos autenticarnos siempre como usuarios y no entrar con el botón "Cancelar". Este proceso se puede automatizar mediante la herramienta **Tweak UI**.

La versión 1.33 de Tweak UI ya está disponible para su descarga e instalación. Tweak UI es un pequeño programa de 110 KB, creado por los ingenieros de Microsoft, que permite modificar características ocultas del interfaz de Windows. Sólo está disponible en inglés.

Cómo acceder a recursos compartidos

Las tres formas más habituales son las siguientes:

Entorno de red (doble clic en Entorno de red). No siempre refleja información actualizada de los ordenadores que están en red. Para que esta información sea lo más fiel posible se requiere tener instalado un servidor de nombres.

Explorador de Windows (botón secundario en Entorno de Red / Explorar; o bien, Menú Inicio / Programas / Explorador de Windows). Este método equivale al anterior, aunque tiene la ventaja de mostrar los recursos compartidos clasificados en forma de árbol.

Buscar PC (botón secundario en Entorno de red / Buscar PC; o bien, Menú Inicio / Buscar / PC). Es el método más eficiente a la hora de localizar ordenadores en la red.

Windows utiliza *nombres UNC* para indicar la ruta de recursos compartidos en la red. Por ejemplo: \\saturno\recurso1\carpeta2 hace referencia a la carpeta "carpeta2" que se encuentra dentro del recurso compartido "recurso1" perteneciente al ordenador "saturno".

Cómo compartir carpetas y unidades de disco

Para que un ordenador pueda compartir carpetas, unidades de disco o impresoras, tiene que haberse configurado antes como servidor. Esto se consigue agregando el servicio "Compartir archivos e impresoras".

Los recursos de red son elementos que pueden ofrecerse (*compartirse*) a otros usuarios de la red. Las carpetas, unidades de disco o impresoras son, por tanto, recursos de red. La forma de compartirlos es similar para todos ellos: botón secundario del ratón sobre el recurso / Compartir.

En el cuadro "Compartir" tenemos que indicar el tipo de acceso (estos tipos de acceso no son aplicables a impresoras):

- Sólo lectura. Otros usuarios de la red sólo podrán ver el contenido del recurso compartido pero no modificarlo.
- Completo. También podrán modificarlo.
- Depende de contraseña. Según la contraseña que escriba el usuario, tendrá un acceso de "Sólo lectura" o "Completo".

Nota: Observe, en el momento de compartir una carpeta, que el nombre del recurso compartido (como lo verán otros usuarios de la red) no tiene porqué coincidir con el nombre de la carpeta (como se verá desde el ordenador local). Es preferible que los nombres de los recursos compartidos no contengan espacios ni caracteres especiales.

Unidades de red

A los usuarios les resulta una tarea incómoda buscar sus archivos dentro de Entorno de red (hay que hacer un elevado número de *clicks* de ratón). Sería interesante que los recursos compartidos apareciesen dentro de "Mi PC" como si fuesen otras unidades más. Esto es justamente lo que deseamos hacer: crear unidades de red (tendrán asignadas letras de unidad) a partir de recursos compartidos.

Nota: Se utiliza el término "unidades de red" para distinguir estas unidades de las "unidades de disco". Una "unidad" se caracteriza por tener asociada una "letra de unidad". En Mi PC se utilizan iconos distintos para una unidad de disco (perteneciente al ordenador local) y para una unidad de red (recurso compartido de otro ordenador de la red).

Hacer clic con el botón secundario del ratón en un recurso compartido y elegir "Conectar a unidad de red".

Seleccionar una letra de unidad (habitualmente se eligen las letras altas del alfabeto, como la X:, Y: o Z:)

Indicar si queremos que esta unidad de red sea permanente o temporal ("Conectar de nuevo al iniciar sesión").

Para eliminar una unidad de red creada con anterioridad elegimos "Desconectar" del menú contextual de la unidad de red.

Cómo instalar una impresora en red

En el servidor de impresión:

Instalar la impresora de forma local y comprobar su funcionamiento. En la pestaña "Detalles" de las propiedades de la impresora indicará un puerto físico (LPT1, por ejemplo).

Compartir la impresora.

En los clientes:

1. Buscar la impresora compartida en Entorno de red.
2. Hacer doble clic en la impresora y seguir los pasos para la instalación.
3. Comprobar en Panel de control / Impresoras que se ha agregado una nueva impresora. En la pestaña "Detalles" de sus propiedades indicará el nombre del recurso compartido de la impresora en red (por ejemplo, \\servidor\epson).

Nota: Para algunos modelos de impresoras el procedimiento anterior no funciona. En estos casos, hay que instalar los drivers del fabricante en cada uno de los ordenadores cliente (como si la impresora estuviese conectada directamente a cada ordenador) y después, cambiar el puerto "LPT1" por un puerto de red "\\servidor\epson".

Nota: En el servidor se instala una "impresora local". En los clientes se instala la "impresora en red" del servidor.

Programas de monitorización de la red

Los programas Monitor de red y Monitor del sistema se encuentran en Menú Inicio / Programas / Accesorios / Herramientas del sistema. Si no apareciesen, se pueden instalar desde Panel de control / Agregar o quitar programas / Instalación de Windows / Herramientas del sistema.

Monitor de red

Controla de forma centralizada el lado servidor de nuestro ordenador y muestra los recursos que está sirviendo a otros usuarios de la red. Desde el menú "Ver" se puede cambiar de vista:

- Por conexiones. Indica los usuarios que están conectados a nuestro ordenador.
- Por carpetas compartidas. Enumera las carpetas y unidades de disco que están compartidas. Para cada recurso compartido muestra los usuarios que están conectados en ese momento. Desde el menú "Administrar" se pueden compartir nuevos recursos o dejar de compartir los que ya lo están.
- Por archivos abiertos. Lista los archivos de nuestro ordenador que están siendo utilizados por otros usuarios de la red.

Monitor del sistema

Muestra estadísticas de forma gráfica. Las gráficas que nos interesan desde el punto de vista de la monitorización de la red son:

- Cliente de Microsoft Network: *Bytes leídos/s*. Tasa de información que estamos recibiendo desde la red.
- Cliente de Microsoft Network: *Bytes escritos/s*. Tasa de información que estamos enviando a la red.
- Servidor de redes Microsoft: *Bytes leídos/s*. Tasa de información que otros usuarios están recibiendo de nuestro ordenador.
- Servidor de redes Microsoft: *Bytes escritos/s*. Tasa de información que otros usuarios están enviando a nuestro ordenador.

Si disponemos de una conexión a Internet por medio de Acceso telefónico a redes, podemos monitorizar la velocidad que tenemos en cada instante:

- Dial-Up Adapter: *Bytes Received/Second*. Velocidad entrante de nuestra conexión a Internet medida en bytes por segundo (si la multiplicamos por 8, tendremos bits por segundo = bps)
- Dial-Up Adapter: *Bytes Transmitted/Second*. Velocidad saliente.

MEJORANDO SU SISTEMA DE RED.



Windows Me facilita las cosas para instalar una red. Ahora usted puede compartir la conexión a Internet, las impresoras, archivos de música y fotografías digitales o jugar juegos frente a frente entre múltiples computadoras en su hogar. Además, es fácil conectar los más modernos dispositivos listos para conectarse, así como demás aparatos a su red casera. Aquí le presentamos algunas de las características que encontrará en Windows Me:

CREAR UNA RED EN CASA.

El proceso para instalar su red casera es simple cuando se utilizan paso a paso las Instrucciones proporcionadas por el Asistente de Red Casera (Home Networking Wizard)

Usted puede fácilmente crear una red utilizando Windows Me. El Asistente de la Red Casera lo lleva a través del proceso paso a paso. El asistente facilita las cosas para que se puedan incluir computadoras ejecutándose en Windows 95 o Windows 98 en su red y para conectar dispositivos periféricos a su red.

Con una red en Windows ME usted puede:

- Compartir una sola conexión a Internet con todas las demás computadoras en su red casera.
- Compartir archivos o documentos multimedia y escoger qué archivos y carpetas compartirá con otras personas de su hogar.
- Trabajar con archivos almacenados en cualquiera de las computadoras de la red.
- Compartir una impresora u otros dispositivos entre todas las PCS.
- Jugar juegos multimedia con otra persona en su hogar.

COMPARTIR UNA SOLA CONEXIÓN A INTERNET.

La opción de Compartir la Conexión a Internet (Internet Connection Sharing; ICS) le permite compartir una sola conexión a Internet entre varias computadoras en su red local, aún si están siendo ejecutadas con Windows 95 o Windows 98.

La característica de Compartiendo una Conexión a Internet (Internet Connection Sharing) en Windows Me le permite compartir una sola conexión a Internet de entre todas las computadoras y dispositivos, basados en Windows, en su red, sin necesidad de tener una conexión separada para cada máquina. La contraseña es "sharing", palabra que significa compartir y que viene a poner orden en cuanto a quién quiere utilizar Internet.

Cuando usted utiliza Internet Connection Sharing:

- Los miembros de la red pueden utilizar Internet al mismo tiempo, ya sea que se esté conectando por medio de una línea telefónica, ADSL o vía cable MODEM.
- Cada computadora puede usar cualesquiera de los servicios de Internet que normalmente usaría si estuviese conectada directamente al Web por sí sola.
- Solamente una PC es visible a su proveedor de servicio de Internet, así que sólo necesita una cuenta para todas sus computadoras.
- Internet esta disponible para los dispositivos Universal Plug and Play en su red casera, tales como teléfonos vía Web, televisiones inteligentes y cajas set-top.
- Configurar Internet Connection Sharing es sencillo utilizando el Asistente de Redes Caseras.

UTILIZAR MÚLTIPLES TECNOLOGÍAS PARA REDES.

Windows Me proporciona soporte para múltiples tipos de tecnologías para redes, incluyendo Ethernet, inalámbrica y homePNA , y, le permite ver estas redes mediante una sola interfaz.

Windows Me proporciona soporte para tecnologías de red existentes, así como también los últimos estándares y tecnologías emergentes. Ahora usted puede aprovechar de las múltiples tecnologías de redes al mismo tiempo. Con Windows Me usted podrá administraras todas mediante una sola, unificada interfaz en su PC.

Las tecnologías y conectividad soportadas por Windows Me incluyen:

- Tecnologías inalámbricas tales como la Asociación de Datos Infrarrojos (Infrared Data Association; IrDa) para conectar computadoras y dispositivos tales como teléfonos celulares, impresoras y computadoras handheld.
- Tipos estándar de Ethernet como son RJ-45 par de cables torcidos y cable coaxial 10Base2.
- IEEE 1394, un bus serial estándar de alta velocidad que proporciona una mayor conexión de ancho de banda para dispositivos que requieren rápida transferencia de datos, tales como cámaras de video digitales.
- HomePNA, una tecnología de redes que utiliza el cableado existente telefónico de su hogar para conectar dispositivos sin interrumpir el servicio telefónico estándar.
- Power Line Carrier (PLC), una tecnología que utiliza la instalación eléctrica casera para transmitir datos.

COMPARTIR RECURSOS A TRAVÉS DE SU RED CASERA.

Windows Me detecta automáticamente impresoras, carpetas y otros recursos en su red local, y le permite compartir fácilmente éstos y otros recursos entre las computadoras de su red.

Una vez que su red local está instalada y activa, continuará creciendo conforme vaya incorporando nuevas computadoras y dispositivos. Windows Me se "toma la molestia" de configurar los recursos en su red y facilita el compartir cualquier dispositivo nuevo a través de su red local. Todo se lleva al cabo automáticamente.

Windows Me lo hace por usted:

- Automáticamente detecta impresoras, cámaras, carpetas y otros recursos existentes en su red casera y le permite compartirlos fácilmente entre todas sus computadoras en red.
- Reconoce cambios que ocurren en el hardware mientras su PC está ejecutándose, tales como conectar una cámara digital o insertar una tarjeta de red, y le da acceso instantáneo a estos dispositivos a través de su red.
- Reconoce nuevo hardware que está instalado en la red entre los reinicios de su PC.

- Soporta estándares de hardware que facilitan el reconocimiento automático de nuevos dispositivos, tales como USB y UPnP.
- Windows Me es el primer sistema operativo en implementar estándares de red UPnP, facilitando la conexión de todo tipo de aparatos de alta tecnología, otros aparatos, dispositivos inalámbricos y computadoras a su red casera.

Windows Me es el primer sistema operativo en implementar estándares para soporte de redes para UPnP. La tecnología UPnP es una iniciativa soportada por Microsoft y más de ochenta empresas líderes en campos tales como los de electrónicos, enseres domésticos, seguridad para el hogar y redes computacionales.

La UPnP define un conjunto de estándares comunes de tecnología que estas compañías utilizarán en el desarrollo de nuevos productos que pueden rápida y fácilmente ser agregados a una red.

El soporte de la tecnología UPnP en Windows Me le permite:

- Conectar y desconectar una amplia matriz de periféricos tales como joysticks, digitalizadores y videocámaras sin tener que configurar o reinicializar su PC.
- Aproveche los beneficios tales como la revelación automática e identificación de recursos en su red, así como la interconexión simplificada entre computadoras, enseres y diversos tipos de redes.
- Puede fácilmente agregar nuevos enseres inteligentes, aparatos y computadoras a su red local conforme vayan saliendo del mercado, sin necesidad de reemplazar la tecnología que ya utiliza en su hogar.
- Está preparado para la siguiente generación de inteligentes dispositivos de red.

CONECTARSE DE FORMA SEGURA AL INTERNET.

La nueva capa TCP/IP en Windows Me proporciona estabilidad mejorada y Seguridad en Internet.

TCP/IP, acrónimo para Protocolo para el Control de la Transmisión/Protocolo de Internet, es el software protocolo para la comunicación entre computadoras en una red. Es ampliamente utilizado en Internet y en redes privadas. Windows Me presenta una enormemente mejorada versión de TCP/IP, basada en la versión encontrada en la versión de la familia de sistemas operativos de Windows 2000.

Las mejoras del TCP/IP en Windows Me proporcionan:

- Mejoras de seguridad y confiabilidad cuando está conectado al Internet.
- Desempeño mejorado, incluyendo tasas de transferencia de datos a mayor velocidad mientras se utiliza Internet.
- Tiempo reducido de la computadora al inicializar.
- Soporte para lo último en tecnologías de redes, incluyendo TCP/IP sobre IEEE 1394, un estándar de transferencia de alta velocidad para dispositivos tales como impresoras, digitalizadores, y HomePNa, una tecnología que proporciona capacidades de red utilizando las líneas telefónicas existentes en casa.

Conclusiones

Para que nos quede todo claro, vamos a dar un pequeño repaso a lo explicado hasta ahora, sabiendo que existe una pequeña variante entre las tres versiones de Windows haciendo cada vez más fácil de configurar y administrar una red.

Nuestra finalidad es compartir recursos, como por ejemplo impresoras a través de la red, esto es, imprimir desde un equipo en la impresora que se instaló en otro equipo. Para ello parece evidente que hemos de conectar físicamente los dos ordenadores.

Hemos escogido el conjunto de protocolos TCP/IP como podríamos haber escogido otros protocolos de red (NetBEUI, etc.). Una vez instalamos los protocolos necesitamos instalar aplicaciones de red y esto lo hemos hecho instalando el Servicio para compartir Archivos e Impresoras. Todo esto lo hemos llevado a cabo sobre Windows. Podríamos haber optado por soluciones diferentes.

La decisión siempre es la misma, elegir un tipo de red, elegir los protocolos a utilizar y elegir el sistema operativo de red. De hecho, esto se suele simplificar a elegir un tipo de red y un sistema operativo de red pues los protocolos y aplicaciones necesarios para el trabajo en red siempre irán incluidos en este.

Cuando estamos pensando en conectar en red una impresora el proceso de razonamiento a seguir es el mismo. En primer lugar hemos de saber a que tipo de redes se puede conectar la máquina, esto depende en gran medida de los conectores de la placa de red de esta. Una impresora de hoy día podrá utilizarse seguramente en una red Ethernet 10base2,10baseT,100baseT.... o TokenRing, este tipo de datos siempre aparece en la documentación de la impresora los mismo pasa con los protocolos soportados y servicios de red soportados.

9. - ADMINISTRACION Y CONFIGURACION DE WINDOWS NT.

MICROSOFT WINDOWS NT.

Microsoft no solo se ha dedicado a escribir software para PCs de escritorio sino también para poderosas estaciones de trabajo y servidores de red y bases de datos.

El sistema operativo Windows NT de Microsoft es un SO para redes que brinda poder, velocidad y nuevas características; además de las características tradicionales. Es un SO de 32 bits, y que puede trabajar en procesadores 486 y Pentium en versiones mas atrasadas.

Además de ser multitarea, multilectura y multiprocesador ofrece una interfaz gráfica. Y trae todo el software necesario para trabajar en redes, permitiendo ser un cliente de la red o un servidor.

9.1. - INTRODUCCIÓN A WINDOWS NT SERVER

Windows NT es un sistema operativo que ayuda a organizar la forma de trabajar a diario con la PC. Las letras NT significan Nueva Tecnología. Fue diseñado para uso de compañías grandes, por lo tanto realiza muy bien algunas tareas tales como la protección por contraseñas. Windows actúa como su ejecutivo personal, personal de archivo, mensajeros, guardias de seguridad, asistentes administrativos y mantenimiento de tiempo completo. Lo que Windows NT no hace bien son los juegos y la multimedia, ya que no ha sido creado para tales usos.

Microsoft Windows NT Server es un sistema operativo diseñado para su uso en servidores de red de área local (LAN). Ofrece la potencia, la manejabilidad y la capacidad de ampliación de Windows NT en una plataforma de servidor e incluye características, como la administración centralizada de la seguridad y tolerancia a fallos más avanzada, que hacen de él un sistema operativo idóneo para servidores de red.

Windows NT Server es a la vez un sistema operativo para computadoras (ordenadores) personales y un sistema operativo para red. Puesto que incorpora funciones de red, las redes de Windows NT Server se integran de forma óptima con el sistema operativo básico, facilitando el uso y la administración de las funciones.

9.2 .- DESCRIPCIÓN GENERAL DE WINDOWS NT SERVER.

Windows NT Server es un sistema operativo para servidores, ampliable e independiente de la plataforma. Puede ejecutarse en sistemas basados en procesadores Intel x86, RISC y DEC Alpha, ofreciendo al usuario mayor libertad a la hora de elegir sus sistemas informáticos. Es ampliable a sistemas de multiproceso simétrico, lo que permite incorporar procesadores adicionales cuando se desee aumentar el rendimiento.

Internamente posee una arquitectura de 32 bits. Su modelo de memoria lineal de 32 bits elimina los segmentos de memoria de 64 KB y la barrera de 640 KB de MS-DOS.

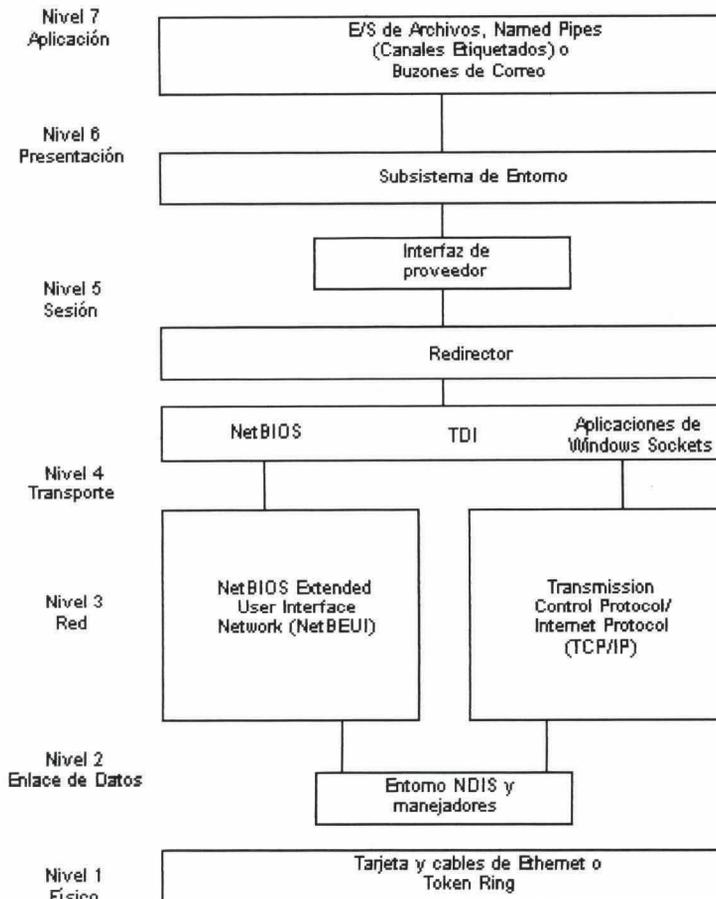
Posee múltiples threads (subprocesos) de ejecución, lo que permite utilizar aplicaciones más potentes. La protección de la memoria garantiza la estabilidad mediante la asignación de áreas de memoria independientes para el sistema operativo y para las aplicaciones, con el fin de impedir la alteración de los datos. La capacidad de multitarea de asignación prioritaria permite al sistema operativo asignar tiempo de proceso a cada aplicación de forma eficaz.

Windows NT Server incluye, asimismo, diversas funciones de red, que se describen brevemente en las siguientes secciones y con más detalle en capítulos posteriores de esta tesis.

9.3. - ARQUITECTURA DE REDES ABIERTAS.

Windows NT Server es compatible con los estándares NDIS (Especificación de la interfaz del controlador de red) y TDI (Interfaz del controlador de transporte). NDIS es una interfaz estándar para comunicación entre controladores de tarjetas adaptadoras de red y protocolos de red. NDIS le permite combinar y coordinar tarjetas y protocolos de red sin que sea necesario disponer de una versión diferente del protocolo de red para cada tipo de tarjeta. Permite también utilizar varios protocolos en una misma tarjeta de red. Con Windows NT Server se suministran cuatro protocolos compatibles con el estándar NDIS: TCP/IP, Microsoft NWLink, NetBEUI y DLC (Control de vínculos de datos).

La interfaz TDI se comunica entre el protocolo de red y el software de red de alto nivel (como el servidor y el redirector). TDI elimina la necesidad de que el redirector y el servidor se comuniquen directamente con los protocolos de red, o de tener información de los mismos, permitiendo de esta forma utilizar protocolos, servidores o redirectores diferentes con Windows NT Server. También es compatible con aplicaciones de RPC (Llamada a procedimientos remotos), aplicaciones de sistema de entrada/salida básico de red (NetBIOS) y aplicaciones con Windows Sockets.



Arquitectura De Windows NT Con Advanced Server.

Seguridad incorporada

Windows NT Server incorpora la seguridad en el sistema operativo. El control de acceso discrecional le permite asignar permisos a archivos individuales. El concepto de derechos de usuario le ofrece un sistema de control discrecional de las funciones básicas del sistema, como establecer la hora y cerrar la computadora. Se incluyen, asimismo, funciones completas de auditoría.

Windows NT Server permite crear dominios y establecer relaciones de confianza, con el fin de centralizar las cuentas de usuario de la red y otro tipo de información de seguridad, facilitando el uso y la administración de la red. Con una administración centralizada de la seguridad, sólo es necesario administrar una cuenta por cada usuario. Dicha cuenta permite al usuario acceder a todos los recursos de la red.

9.4 .- REGISTRO DE CONFIGURACIÓN.

Windows NT Server y Windows NT Workstation mantienen una base de datos denominada Registro. Esta base de datos contiene información acerca del sistema operativo, de la computadora y de los usuarios que anteriormente hayan iniciado sesiones en esta computadora. Las aplicaciones que detecten la presencia de Windows NT podrán almacenar en el Registro la información de inicialización.

El Registro reemplaza la necesidad de separar los archivos de configuración. Sin embargo, para ser compatible con aplicaciones escritas para utilizar CONFIG.SYS y AUTOEXEC.BAT, Windows NT automáticamente mantiene y usa versiones de estos archivos que contienen solamente la información de la aplicación.

Administración de las estaciones de trabajo de los usuarios.

Los perfiles de usuario de Windows NT Server le permiten proporcionar mayor facilidad de uso a los usuarios y al mismo tiempo restringir sus actividades en las estaciones de trabajo. Si desea utilizar perfiles para aumentar la productividad de los usuarios, puede guardar en los servidores un perfil con la configuración y las preferencias de los usuarios, tales como las conexiones de red, los grupos de programas e incluso los colores de la pantalla. Este perfil se utilizará cada vez que el usuario inicie una sesión en cualquier computadora con Windows NT, de forma que el entorno definido por el usuario le siga de una estación de trabajo a otra.

Si desea utilizar los perfiles de usuario para limitar las actividades de los usuarios, deberá agregar restricciones al perfil, como por ejemplo, impedir que el usuario cambie los grupos y los elementos de programas que usted haya definido, o inhabilitar parte de la interfaz de Windows NT cuando el usuario haya iniciado una sesión.

Monitorización del rendimiento.

Windows NT Server incluye también una sofisticada aplicación que permite monitorizar el rendimiento. Puede utilizar esta herramienta para observar, representar gráficamente y registrar cientos de datos estadísticos acerca de tipos específicos de rendimiento, agrupados en categorías generales tales como tráfico entre servidores de la red, rendimiento de los discos, uso de los procesadores, y estadísticas de los servidores y las estaciones de trabajo.

El Monitor de sistema le permite supervisar simultáneamente el rendimiento de un gran número de computadoras remotas, de forma que pueda controlar y comparar simultáneamente el rendimiento y el uso de un gran número de servidores.

Seguimiento de la actividad de la red.

Windows NT Server proporciona numerosas herramientas para realizar el seguimiento de la actividad y el uso de la red. Puede observar los servidores y examinar qué recursos están compartiendo, ver qué usuarios están conectados a un servidor de la red y observar qué archivos tienen abiertos, registrar y ver las anotaciones de auditoría de seguridad, mantener registros de error exhaustivos y especificar las alertas que se deben enviar a los administradores en caso de que se produzcan determinados sucesos. Si su red utiliza el protocolo TCP/IP, podrá emplear también la utilidad de administración SNMP, suministrada con Windows NT Server.

9.5 .- VENTAJAS DE WINDOWS NT.

- La instalación es muy sencilla y no requiere de mucha experiencia.
- Es multitarea y multiusuario.
- Apoya el uso de múltiples procesadores.
- Soporta diferentes arquitecturas.
- Permite el uso de servidores no dedicados.
- Soporta acceso remoto, ofreciendo la detección de intrusos, y mucha seguridad en estas sesiones remotas.
- Apoyo para archivos de DOS y MAC en el servidor.
- El sistema está protegido del acceso ilegal a las aplicaciones en las diferentes configuraciones.
- Permite cambiar periódicamente las contraseñas.
- Soporta múltiples protocolos.
- Carga automáticamente manejadores en las estaciones de trabajo.
- Trabaja con impresoras de estaciones remotas.
- Soporta múltiples impresoras y asigna prioridades a las colas de impresión.
- Muestra estadísticas de Errores del sistema, Caché, Información Del disco duro, Información de Manejadores, Nº de archivos abiertos, Porcentaje de uso del CPU, Información general del servidor y de las estaciones de trabajo, etc.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar diferentes tipos de auditorías, tales como del acceso a archivos, conexión y desconexión, encendido y apagado del sistema, errores del sistema, información de archivos y directorios, etc.
- No permite criptografía de llave pública ni privada.
- No permite realizar algunas tareas en sesiones remotas, como instalación y actualización.

Desventajas de Windows NT.

- Tiene ciertas limitaciones por RAM, como: N° Máximo de archivos abiertos y almacenamiento de disco total.
- Requiere como mínimo 16 Mb en RAM y un procesador Pentium de 133 MHz o uno superior.
- El usuario no puede limitar la cantidad de espacio en el disco duro.
- No soporta archivos de NFS.
- No ofrece el bloqueo de intrusos.
- No soporta la ejecución de algunas aplicaciones para DOS.

Fallas.

Aparte de los problemas con los manejadores de hilos y otras aplicaciones, encontramos que es particularmente frustrante la falta de una documentación adecuada que pueda prevenir totalmente una falla.

Podríamos hacer una conexión y utilizar el IP bajo un modo nivelado con utilidades «Ping» al igual que «FTP», pero cualquier intento por ver archivos compartidos e impresores fallaron. Encontramos documentación para muchos nuevos rasgos en particular, para la asignación «Built-In» que es para la asignación de ruta del multiprotocolo y la garantía de IP está completamente inadecuada.

Los cambios que presenta la versión revisada de Windows NT son significativos en cuanto a las diferencias que presentan con las versiones anteriores. Las combinaciones de Windows NT nos proporcionan mejoras en cuanto a la ejecución, proporcionan rasgos nuevos y los usuarios cuentan con la versión revisada de Windows NT 3.x.

9.5 .- PRINCIPALES CARACTERÍSTICAS.

- Es nueva tecnología para el mundo de las PC y es diferente por su ambiente gráfico, pero realmente no es nueva tecnología.
- Está basado en variaciones del kernel de Mac de UNIX. La arquitectura del microkernel soporta aplicaciones no diseñadas para Windows NT.
- Operaciones básicas de sistemas y otras capas sobre ella.
- Soporta 5 subsistemas: Windows 32 bits / Windows 16 bits / DOS / POSIX / OS/2.
- Funciona como Cliente – Servidor en un ambiente de red.
- Permite desarrollar servicios de redireccionamiento para LAN Manager de Mips, RISC y Digital Alpha.
- Soporta sistemas de multiproceso.
- Cada aplicación se encuentra ejecutando en un hilo tratado como una caja multiprocesadora.
- Al igual que OS/2 ejecuta aplicaciones con errores de codificación, principalmente al ejecutarse en procesadores 386 y 486.
- Cada aplicación es limitada a un espacio de memoria (Esquema de direccionamiento de 32 bits real). Ejecuta aplicaciones de 16 y 32 bits y de otros Sistemas Operativos y para RISC de 64 bits.
- Existe una versión para Laptop.
- Soporta la tecnología Plug-in para sistemas API y sistemas de archivos instalables.
- También cuenta con servicios básicos de redes y APIs para archivos, manejadores de impresión, manejo de mensajes y seguridad directa. Aplicaciones para redes digitales que pueden ejecutarse en diferentes plataformas.
- Implanta facilidades para el uso de OSF, DCE y RPCs.
- Para facilitar los puertos de aplicación aísla el kernel del Hardware (Tipo de interfaz para el Sistema Operativo), con lo que se logra la portabilidad o compatibilidad a nivel de código.
- Provee datos, aplicaciones y protección del sistema contra accesos inadvertidos.

- Permite a los usuarios un acceso seguro a más información sin comprometer la seguridad del sistema.
- Conserva las principales características del servidor 3.51 incluso el protocolo nativo NetBEUI, IPX y TCP/IP.
- Soporta hasta 256 usuarios, administración de multidominio y replicación de directorio.
- Nuevas o mejoradas herramientas de administración y perfeccionamiento en la ejecución.
- El servidor NT relacionado con Internet, envía la información con el servidor de Internet IIS versión 2.0. También hace uso del FTP. Relaciona nuevos rasgos punto a punto con el protocolo PPTP y TCP/IP.
- Ayuda a consolidar la posición de NT como la plataforma del servidor en escenarios de Internet.
- Adopta el estilo de Unix de servicio de dominio DNS como norma.
- Incluye herramientas basadas en el Web referentes a la administración.
- VISIÓN GENERAL.

Seguridad.

Windows NT ofrece gran seguridad por medio del acceso por cuentas y contraseñas. Es decir un usuario debe tener su cuenta asignada y una contraseña para poder tener acceso al sistema.

Contiene protecciones para directorios, archivos, y periféricos, es decir que todo esto se encuentra con una contraseña para poder ser utilizados.

CONCEPTO DE DERECHOS: Permite a un grupo de usuarios efectuar determinadas operaciones.

CUENTA ADMINISTRADOR: Controla todos los permisos y con ellas se puede: dar de alta; asignar cuentas; cancelar derechos

Comunicación: Permite acceder y compartir discos en red.

Permite compartir archivos, directorios y periféricos.

9.7 FUNCIONAMIENTO DE LA SEGURIDAD EN LA RED.

Windows NT Server incorpora diversos métodos de seguridad. Estos métodos proporcionan numerosas formas de controlar la actividad de los usuarios, sin impedirles por ello el acceso a los recursos que necesitan. El fundamento de la seguridad de Windows NT es que todos los recursos y acciones están protegidos por el control de acceso discrecional, que significa que es posible permitir a determinados usuarios acceder a un recurso o realizar una determinada acción, y al mismo tiempo impedirselo a otros usuarios. Además, la seguridad es muy granular

Con Windows NT Server, la seguridad está integrada en el sistema operativo desde el principio, en lugar de incorporarse al mismo como un componente adicional. Esto significa que los archivos y otros recursos pueden protegerse incluso de los usuarios que trabajan en la misma computadora donde se encuentre el recurso, así como de los usuarios que accedan al recurso a través de la red. Windows NT Server incorpora medidas de seguridad incluso para las funciones básicas del sistema, como el propio reloj de la computadora.

Windows NT Server ofrece asimismo un modelo lógico de administración que permite administrar de un modo eficaz una red de gran tamaño. Cada usuario sólo necesita disponer de una única cuenta, que se almacena de modo centralizado. Esta única cuenta puede proporcionar al usuario el acceso a cualquier recurso de la red, independientemente del lugar donde se encuentre.

- Soporta servicios básicos de redes de trabajo: Manejadores de impresión; Manejo de mensajes.
- Seguridad directa.
- Tienen soporte para sistemas distribuidos y concurrencia real.

Funcionamiento de Windows NT Server con otro software de red.

Windows NT Server está diseñado para su uso en servidores de grandes redes. Funciona de forma óptima con otros sistemas operativos de red fabricados por Microsoft. Windows NT Workstation es el sistema operativo más adecuado para los clientes que precisen altos rendimientos de la red. Windows NT Workstation está diseñado para usuarios avanzados, desarrolladores de software y para aplicaciones críticas; además, traslada al escritorio muchas de las funciones de seguridad de Windows NT Server. Al igual que ocurre en Windows NT Server, tanto la seguridad como las funciones de red están integradas en el sistema operativo.

Windows NT Server también es compatible con los sistemas Microsoft LAN Manager 2.x. Las computadoras que funcionen bajo MS-DOS, Windows 3.1 y OS/2 que posean software para estaciones de trabajo LAN Manager pueden acceder a servidores en los que se ejecute Windows NT Server. Los servidores de LAN Manager 2.x (tanto en sistemas OS/2 como UNIX) pueden funcionar con servidores en los que se esté ejecutando Windows NT Server, incluso en el mismo dominio.

La Conexión con Internet.

Windows NT también hace uso del FTP que es nativo del WEB. Este le permite introducir los nuevos rasgos punto a punto que están relacionados con Internet, al igual que con el protocolo PTPP y el TCP / IP esto puede ayudar a consolidar la posición de NT como la plataforma del servidor de Internet. Microsoft adopta finalmente el estilo de UNIX referente a los dominios y lo implanta como una norma. Es sencillo hacer uso de éste, únicamente basta con nombrar el servicio DNS.

Puede teclear ahora en DNS el nombre del dominio y se conseguirá que el IP se dirija automáticamente, además se reconocerán los nombres válidos, aunque el funcionamiento del DNS es un poco arrogante, el organizador lo tiene disponible.

Sistemas de Archivos.

Tiene 3 diferentes tipos y uno nuevo desarrollado por NT. Los primeros 3 son para compatibilidad: FAT para DOS; HPFS para OS/2; CDFS se usa para acceder discos compactos; NTFS es el sistema de archivos propio de Windows NT, el cual está basado en un sistema de transacciones, es decir que tiene la capacidad de almacenar una gran cantidad de operaciones a disco para que en el caso de alguna falla este elemento pueda ser usado para la reconstrucción del sistema de archivos del disco.

Multitarea

Para la ejecución simultánea de múltiples tareas NT utiliza: Manager; Scheduler; Manejador de excepciones e interrupciones. Mecanismos de sincronización. El usuario puede dejar ejecutando alguna tarea en una ventana y seguir trabajando en otra.

Memoria Virtual.

NT tiene un manejador de memoria virtual que permite el uso de un espacio de direccionamiento de 2 GB. Este espacio de direccionamiento está protegido de otros procesos del sistema. Traduce direcciones virtuales a direcciones físicas. Y también se encarga del problema de traer y llevar páginas de disco a memoria y de memoria a disco.

Protocolos que Soporta.

- NetBEUI.
- TCP/IP.
- IPX/SPX.
- Banyan
- DECnet.
- Apple Talk.
- Ventajas de NDIS.

DIS ofrece un conjunto de normas para la comunicación entre protocolos y controladores de tarjetas adaptadoras. Así, en cualquier estación de trabajo podrá utilizarse cualquier combinación de controladores de protocolo compatibles con NDIS junto con cualquier controlador de tarjeta adaptadora de red compatible con NDIS.

Es probable que las computadoras existentes en su red tengan distintos tipos de tarjetas adaptadoras de red, por lo que necesitará distintos controladores de tarjetas adaptadoras de red. Gracias al estándar NDIS, podrá utilizar exactamente el mismo controlador de protocolo en todas sus estaciones de trabajo, sin necesidad de disponer de una versión diferente del protocolo para cada tarjeta adaptadora de red, como sucedería si utilizase pilas de protocolos monolíticas.

Con Windows NT las tarjetas inteligentes apenas representan una ventaja, ya que es Windows NT, con sus controladores, quien realiza la mayor parte del trabajo de procesamiento relacionado con la red.

Además, NDIS permite que varios protocolos utilicen una misma tarjeta de red. Normalmente, cuando se utiliza un protocolo monolítico con una tarjeta adaptadora de red, dicho protocolo monopoliza la tarjeta de red, impidiendo la utilización de otros protocolos con dicha tarjeta.

En una computadora con Windows NT, cada uno de los enlaces entre un protocolo y una tarjeta adaptadora de red tiene asignado un número de adaptador de red local. Cuando instale Windows NT en una computadora, Windows NT asignará automáticamente números de adaptador de red local a los enlaces entre protocolos y tarjetas adaptadoras de red. Sólo necesitará cambiar estos números de adaptador de red local si tiene alguna aplicación NetBIOS que exija la utilización de un determinado número de adaptador de red local.

Microsoft ofrece cuatro protocolos para utilizar con Windows NT: TCP/IP, NWLink, NetBEUI y DLC (Control de vínculo de datos). Debe elegir el modo en que se utilizará uno o varios de estos protocolos en su red. En las siguientes secciones se indican el uso, las ventajas y desventajas de cada uno de ellos.

Funcionamiento de TCP/IP.

TCP/IP son las siglas en inglés de Protocolo de control de transmisión/Protocolo Internet. Fue desarrollado a finales de los años 70, como resultado de un proyecto de investigación sobre interconexión de redes realizado por la Agencia de proyectos de investigación avanzada para la defensa (DARPA) de Estados Unidos. La principal ventaja y utilidad de TCP/IP es que es un protocolo estándar y reencaminable; se trata del protocolo más completo y aceptado de todos los existentes. Permite comunicarse a través de redes interconectadas con distintos sistemas operativos y arquitecturas de hardware, como UNIX o computadoras principales, así como con Windows NT.

TCP/IP ofrece además compatibilidad con Internet, un conjunto de redes y pasarelas (gateways) interconectadas que vinculan numerosas universidades, empresas, organismos gubernamentales e instalaciones militares de todo el mundo. Además, TCP/IP es necesario para poder utilizar el sistema de administración de red SNMP (Protocolo simple para la administración de redes). SNMP puede utilizarse para monitorizar cualquier computadora con Windows NT que utilice TCP/IP como protocolo principal o como protocolo adicional.

TCP/IP ofrece la interfaz de Windows Sockets 1.1, un marco multiplataforma cliente-servidor que resulta idóneo para desarrollar aplicaciones cliente-servidor que puedan funcionar con pilas de otros fabricantes que se ajusten a Windows Sockets. Las aplicaciones Windows Sockets pueden aprovechar otros protocolos de red, como Microsoft NWLink.

TCP/IP de Microsoft utiliza también la interfaz de NetBIOS, comúnmente conocida como Petición para comentarios (RFC) de NetBIOS. Además, Microsoft proporciona diversas utilidades TCP/IP para su uso con TCP/IP en Windows NT.

Es el protocolo más aceptado, aunque no es tan rápido como NetBEUI en redes locales de pequeño tamaño.

Funcionamiento de NetBEUI.

NetBEUI (Interfaz extendida de usuario de NetBIOS) fue presentado por primera vez por IBM en 1985. NetBEUI es un protocolo compacto, eficiente y rápido.

En 1985, cuando fue desarrollado el protocolo NetBEUI, se consideró que las redes locales estarían segmentadas en grupos de trabajo de entre 20 y 200 computadoras y que se utilizarían pasarelas (gateways) para conectar cada segmento de red local con otro segmento de red local, o con una computadora principal.

NetBEUI está optimizado para obtener un rendimiento muy elevado cuando se utiliza en redes locales o segmentos de redes locales departamentales. En cuanto al tráfico cursado dentro de un segmento de red local, NetBEUI es el más rápido de los protocolos suministrados con Windows NT.

En sentido estricto, NetBEUI 3.0 no es realmente NetBEUI, sino más bien un protocolo con formato de trama de NetBIOS (NBF). NetBEUI utiliza la interfaz NetBIOS como su interfaz de nivel superior, mientras que NBF se ajusta al estándar de Interfaz de controlador de transporte (TDI). (Si desea obtener más información sobre TDI, consulte la sección "Concepto de nivel TDI", más adelante en este mismo capítulo). No obstante, NBF es totalmente compatible e interoperable con el NetBEUI incluido en productos anteriores de red de Microsoft y, en las pantallas de Windows NT, se hace referencia a él como NetBEUI.

Fue concebido expresamente para la comunicación dentro de redes locales pequeñas y, por lo tanto, es muy rápido. Tiene buena protección frente a errores y utiliza poca memoria. Sin embargo, no admite encadenamientos y su rendimiento en redes de área amplia (WAN) es pobre.

Puesto que NetBEUI es muy rápido para comunicaciones dentro de redes locales de pequeño tamaño, pero su rendimiento es peor para las comunicaciones con redes de área amplia (WAN), un método recomendable para configurar una red es utilizar NetBEUI y otro protocolo, como TCP/IP, en cada una de las computadoras que necesiten acceder a otras computadoras a través de un encaminador o una red de área amplia.

Funcionamiento de DLC (Control de vínculo de datos).

A diferencia de NetBEUI y TCP/IP, el protocolo DLC no ha sido diseñado para servir de protocolo principal entre PC. Por el contrario, se suele utilizar DLC con Windows NT si se necesita que las computadoras con Windows NT accedan a computadoras principales IBM o si se está configurando una impresora que se conecta directamente a un cable de red.

Si se desea utilizar DLC para permitir la comunicación entre computadoras con Windows NT y computadoras principales, bastará con añadir el protocolo DLC como protocolo adicional en cada una de las computadoras que se comunican realmente con las computadoras principales. No será necesario que instale DLC en todas las computadoras de la red.

A diferencia de los otros protocolos de Windows NT, como NetBEUI o TCP/IP, el protocolo DLC no se encuadra dentro de los niveles de redes o de transporte del modelo de referencia OSI, sino que ofrece a los programas de alto nivel una interfaz directa con el nivel de vínculos de datos.

Configuración de RPC.

Windows NT permite utilizar aplicaciones distribuidas basadas en RPC (Llamada a procedimientos remotos). Microsoft RPC consta de un conjunto de servicios y bibliotecas de tiempo de ejecución que permiten ejecutar bajo Windows NT una aplicación distribuida. Una aplicación distribuida consta de múltiples procesos que colaboran para llevar a cabo una determinada tarea. Estos procesos pueden estar ejecutándose en una misma computadora o en varias diferentes.

Microsoft RPC utiliza un proveedor de servicio de nombres para localizar y registrar los servidores de la red. Los proveedores de servicio de nombres para Microsoft RPC deben ajustarse al estándar NSI (Interfaz de servicio de nombres) de Microsoft RPC. NSI consta de un conjunto de funciones de la API (Interfaz de programación de aplicaciones) que permiten el acceso y la manipulación de una base de datos del servicio de nombres. Una base de datos de servicio de nombres es una base de datos que contiene entradas para servidores, para grupos y para perfiles.

9.8 .- DOMINIOS Y RELACIONES DE CONFIANZA.

La administración de una red local bajo Windows NT se basa en los dominios y relaciones de confianza.

La unidad básica de la administración centralizada y la seguridad en Windows NT Server es el dominio. Un dominio es un grupo de servidores que ejecutan Windows NT Server y que, en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT Server de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que sólo es necesario escribir una vez la información de una cuenta de usuario para que todos los servidores del dominio reconozcan dicha cuenta.

Dentro de los servidores de un dominio existen dos jerarquías: el servidor PDC (Primary Domain Controller) y los servidores BDC (Backup Domain Controller). Por cada dominio ha de haber un PDC y sólo uno, y posiblemente varios BDC. Cuando el administrador del dominio da de alta un nuevo usuario, lo hace sobre el PDC. Los datos sobre los usuarios se guardan en una base de datos llamada SAM, que la tiene cualquier servidor. El PDC se encarga de copiar esa base de datos de usuarios a todos los BDCs de su dominio de manera periódica. Con sólo dar de alta un usuario en el PDC, ese usuario automáticamente puede acceder a cualquier servidor del dominio y además usando el mismo nombre de usuario y la misma palabra de paso. Este proceso de copia periódica de la SAM se denomina replicación.

Los dominios de una red se relacionan mediante el concepto de Trust o Relación de Confianza. Se dice que un dominio A confía en otro B, o que hay establecida una relación de confianza desde A hacia B, cuando cualquier usuario autorizado en el dominio B puede entrar sin más en el dominio A. Esta relación de confianza son vínculos entre dominios, que permiten realizar una autenticación transparente, en virtud de la cual un usuario sólo poseerá una cuenta de usuario en un dominio pero podrá acceder a toda la red.

Un grupo local es un grupo de usuarios, de manera que cualquier usuario del grupo puede entrar y acceder a los recursos del servidor PDC del dominio al que pertenece el grupo. Un grupo local se define como perteneciente a un dominio.

Un grupo global es igual que el anterior excepto en que puede ser visto también por todos los dominios que confían en el dominio al que pertenece el grupo. La diferencia entre local y global es, pues, el ámbito de visibilidad. Si A confía en B, y definimos en B un grupo global, entonces ese grupo también se puede utilizar en A.

Dominios: unidades administrativas básicas.

La agrupación de computadoras en dominios proporciona dos grandes ventajas a los usuarios y administradores de la red. Lo que es más importante, los servidores de un dominio constituyen una unidad administrativa única que comparte la información de seguridad y de cuentas de usuario. Cada dominio posee una base de datos que contiene las cuentas de los usuarios y grupos, y las configuraciones del plan de seguridad. Todos los servidores del dominio que funcionen como controlador principal de dominio o como controlador de reserva mantendrá una copia de esta base de datos.

La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observará que está agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo

Nota: No debe confundirse el concepto de dominio de Windows NT Server con los dominios del protocolo de red TCP/IP. Un dominio TCP/IP describe parte de la Internet TCP/IP y no tiene nada que ver con los dominios de Windows NT Server.

- Relaciones de confianza: vínculos entre dominios.

Estableciendo relaciones de confianza entre los dominios de la red, se permitirá que determinadas cuentas de usuario y grupos globales puedan utilizarse en dominios distintos de aquél en el que estén situadas dichas cuentas.

Ello facilita en gran medida la administración, ya que cada cuenta de usuario tiene que crearse una sola vez para toda la red. Además, ofrece la posibilidad de acceder a cualquier computadora de la red y no únicamente a las computadoras de uno de los dominios.

Cuando se establezca una relación de confianza entre dominios, uno de los dominios (el dominio que confía) confiará en el otro (el dominio en el cual se confía). A partir de entonces, el dominio que confía reconocerá a todos los usuarios y cuentas de grupo globales del dominio en el cual se confía. Estas cuentas podrán utilizarse como se desee dentro del dominio que confía; podrán iniciar sesiones en estaciones de trabajo situadas en el dominio que confía, integrarse en grupos locales dentro de dicho dominio, y recibir permisos y derechos dentro de ese dominio.

Las relaciones de confianza pueden ser unidireccionales o bidireccionales. Una relación de confianza bidireccional es simplemente un par de relaciones unidireccionales, en virtud del cual cada dominio confía en el otro.

El requisito mínimo de un dominio es un servidor con Windows NT Server, que actúa como controlador principal de dominio y que almacena la copia principal de la base de datos de grupos y usuarios del dominio. Si se desea, un dominio puede incluir también otros servidores adicionales que actúen como controladores de reserva.

- Controlador principal de dominio.

El controlador principal de dominio de un dominio de Windows NT Server debe ser un servidor que ejecute Windows NT Server. Cualquier modificación a la base de datos de grupos y usuarios del dominio deberá realizarse en la base de datos que está almacenada en el controlador principal de dominio. El Administrador de usuarios para dominios no permite modificar directamente la base de datos de usuarios de un servidor de dominio que no sea el controlador principal de dominio.

- Controladores de reserva.

Los controladores de reserva que ejecuten Windows NT Server almacenarán también copias de la base de datos de cuentas del dominio. La base de datos de cuentas del dominio estará duplicada en todos los controladores de reserva del dominio.

Todos los controladores de reserva, además del controlador principal de dominio, podrán procesar las peticiones de inicio de sesión por parte de las cuentas de usuario del dominio. Cuando el dominio reciba una petición de inicio de sesión, el controlador principal de dominio o cualquier controlador de reserva podrá autenticar el intento de inicio de sesión. Es conveniente que en un dominio haya uno o varios controladores de reserva, además del controlador principal de dominio. Estos servidores adicionales proporcionan un mecanismo de seguridad: si el controlador principal de dominio no está disponible, un controlador de reserva podrá ser promovido al puesto de controlador principal de dominio, lo cual permitirá al dominio seguir funcionando. La existencia de varios controladores de dominio permite también distribuir la carga de trabajo relacionada con las peticiones de inicio de sesión, lo cual resulta especialmente útil en dominios con un gran número de cuentas de usuario.

Si en un dominio hay varios servidores que ejecutan Windows NT Server, uno de ellos será el controlador principal de dominio. Debe configurar al menos otro servidor como controlador de reserva. Si el dominio tiene servidores situados en distintas ubicaciones físicas conectadas mediante un vínculo de red de área amplia (WAN), cada ubicación deberá tener al menos un controlador de reserva.

- Servidores.

Además de los controladores principales y de reserva de dominio, existe otro tipo de servidor que ejecuta Windows NT Server. Se trata de servidores designados como "servidores", no como controladores de dominio. Estos servidores pueden participar en un dominio, si bien no es necesario. Un servidor que participa en un dominio no consigue realmente una copia de la base de datos de usuarios del dominio, pero tiene acceso a todas las ventajas de la base de datos de usuarios y grupos del dominio.

Un servidor que no participa en ningún dominio sólo tiene su propia base de datos de usuarios y procesa por su cuenta las peticiones de inicio de sesión. No comparte la información sobre cuentas con ninguna otra computadora y no puede utilizar cuentas de ningún otro dominio.

Si es posible que el servidor se mueva a otro dominio en el futuro. Es más sencillo mover un servidor de un dominio a otro que mover un controlador de reserva de un dominio a otro.

9.9 .- ARQUITECTURA DEL SISTEMA.

- **Introducción.**

Windows NT presenta una arquitectura del tipo cliente-servidor. Los programas de aplicación son contemplados por el sistema operativo como si fueran clientes a los que hay que servir, y para lo cual viene equipado con distintas entidades servidoras.

Los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro-kernel

Por tanto en un primer acercamiento a la arquitectura se distingue un núcleo que se ejecuta en modo privilegiado, y se denomina Executive, y unos módulos que se ejecutan en modo no privilegiado, llamados subsistemas protegidos.

Los programas de usuario (también llamados programas de aplicación) interaccionan con cualquier sistema operativo (S.O. en adelante) a través de un juego de llamadas al sistema propio de dicho sistema. En el mundo Windows en general, las llamadas al sistema se denominan API (Application Programming Interfaces, interfaces para la programación de aplicaciones).

- Los subsistemas protegidos.

Son una serie de procesos servidores que se ejecutan en modo no privilegiado, al igual que los procesos de usuario, pero que tienen algunas características propias que los hacen distintos.

Se inician al arrancar el S.O. y existen dos tipos: integrales y de entorno.

Un subsistema integral es aquel servidor que ejecuta una función crítica del S.O. (como por ejemplo el que gestiona la seguridad). Un subsistema de entorno da soporte a aplicaciones procedentes de S.O. distintos, adaptándolas para su ejecución bajo Windows NT. Existen tres de este tipo:

- Win32, que es el principal, y proporciona la interfaz para aplicaciones específicamente construidas para Windows NT.
- POSIX, que soporta aplicaciones UNIX.
- OS/2, que da el entorno a aplicaciones procedentes del S.O. del mismo nombre.
- El subsistema Win32.

Es el más importante, ya que atiende no sólo a las aplicaciones nativas de Windows NT, sino que para aquellos programas no Win32, reconoce su tipo y los lanza hacia el subsistema correspondiente. En el caso de que la aplicación sea MS-DOS o Windows de 16 bits (Windows 3.11 e inferiores), lo que hace es crear un nuevo subsistema protegido. Así, la aplicación DOS o Win16 se ejecutaría en el contexto de un proceso llamado VDM (Virtual DOS Machine, máquina virtual DOS), que no es más que un simulador de un ordenador funcionando bajo MS-DOS. Las llamadas al API Win16 serían correspondidas con las homónimas en API Win32. Microsoft llama a esto WOW (Windows On Win32). El subsistema soporta una buena parte del API Win32. Así, se encarga de todo lo relacionado con la interfaz gráfica con el usuario (GUI), controlando las entradas del usuario y salidas de la aplicación.

- El subsistema POSIX.

La norma POSIX (Portable Operating System Interface for UNIX) fue elaborada por IEEE para conseguir la portabilidad de las aplicaciones entre distintos entornos Windows NT, UNIX, VMS, etc. Se trata de un conjunto de 23 normas, identificadas como IEEE 1003.0 a IEEE 1003.22, o también POSIX.0 a POSIX.22, de las cuales el subsistema POSIX soporta la POSIX.1, que define un conjunto de llamadas al sistema en lenguaje C. El subsistema sirve las llamadas interaccionando con el Executive.

- El subsistema OS/2.

Igual que el subsistema POSIX proporciona un entorno para aplicaciones UNIX, este subsistema da soporte a las aplicaciones del S.O. OS/2. Proporciona la interfaz gráfica y las llamadas al sistema; las llamadas son servidas con ayuda del Executive.

- El subsistema proceso de inicio.

El proceso de inicio (Logon Process) recibe las peticiones de conexión por parte de los usuarios. En realidad son dos procesos, cada uno encargándose de un tipo distinto de conexión: el proceso de inicio local, que gestiona la conexión de usuarios locales directamente a una máquina Windows NT; y el proceso de inicio remoto, el cual gestiona la conexión de usuarios remotos a procesos servidores de NT.

- El subsistema de seguridad.

Este subsistema interacciona con el proceso de inicio y el llamado monitor de referencias de seguridad, de esta forma se construye el modelo de seguridad en Windows NT. El subsistema de seguridad interacciona con el proceso de inicio, atendiendo las peticiones de acceso al sistema. Consta de dos subcomponentes: la autoridad de seguridad local y el administrador de cuentas.

El primero es el corazón del subsistema de seguridad, en general gestiona la política de seguridad local, así, se encarga de generar los permisos de acceso, de comprobar que el usuario que solicita conexión tiene acceso al sistema, de verificar todos los accesos sobre los objetos (para lo cual se ayuda del monitor de referencias a seguridad) y de controlar la política de auditorías, llevando la cuenta de los mensajes de auditoría generados por el monitor de referencias. El administrador de cuentas mantiene una base de datos con las cuentas de todos los usuarios (login, claves, identificaciones, etc.).

- El Executive.

No debemos confundir el Executive con el núcleo de Windows NT, aunque muchas veces se usan (incorrectamente) como sinónimos. El Executive consta de una serie de componentes software, que se ejecutan en modo privilegiado, uno de los cuales es el núcleo. Dichos componentes son totalmente independientes

entre sí, y se comunican a través de interfaces bien definidas. En el diseño se procuró dejar el núcleo tan pequeño como fuera posible y, su funcionalidad es mínima.

- El administrador de objetos (Object Manager).

Se encarga de crear, destruir y gestionar todos los objetos del Executive. Se tiene infinidad de objetos: procesos, subprocesos, ficheros, segmentos de memoria compartida, semáforos, mutex, sucesos, etc. Los subsistemas de entorno (Win32, OS/2 y POSIX) también tienen sus propios objetos. Por ejemplo, un objeto ventana es creado (con ayuda del administrador de objetos) y gestionado por el subsistema Win32. La razón de no incluir la gestión de ese objeto en el Executive es que una ventana sólo es innata de las aplicaciones Windows, y no de las aplicaciones UNIX o OS/2. Por tanto, el Executive no se encarga de administrar los objetos relacionados con el entorno de cada S.O. concreto, sino de los objetos comunes a los tres.

- El administrador de procesos (Process Manager).

Se encarga (en colaboración con el administrador de objetos) de crear, destruir y gestionar los procesos y subprocesos. Una de sus funciones es la de repartir el tiempo de CPU entre los distintos subprocesos. Suministra sólo las relaciones más básicas entre procesos y subprocesos, dejando el resto de las interrelaciones entre ellos a cada subsistema protegido concreto. Por ejemplo, en el entorno POSIX existe una relación filial entre los procesos que no existe en Win32, de manera que se constituye una jerarquía de procesos. Como esto sólo es específico de ese subsistema, el administrador de objetos no se entromete en ese trabajo y lo deja en manos del subsistema.

- El administrador de memoria virtual (Virtual Memory Manager).

Windows NT y UNIX implementan un direccionamiento lineal de 32 bits y memoria virtual paginada bajo demanda. El VMM se encarga de todo lo relacionado con la política de gestión de la memoria. Determina los conjuntos de trabajo de cada proceso, mantiene un conjunto de páginas libres, elige páginas víctima, sube y baja páginas entre la memoria RAM y el archivo de intercambio en disco, etc.

- El administrador de entrada/salida (I/O Manager).

Consta de varios subcomponentes: el administrador del sistema de ficheros, el servidor de red, el redirector de red, los drivers de dispositivo del sistema y el administrador de cachés. Buena parte de su trabajo es la gestión de la comunicación entre los distintos drivers de dispositivo, para lo cual implementa una interfaz bien definida que permite el tratamiento de todos los drivers de una manera homogénea, sin preocuparse del funcionamiento específico de cada uno.

Trabaja en conjunción con otros componentes del Executive, sobre todo con el VMM. Le proporciona la E/S síncrona y asíncrona, la E/S a archivos asignados en memoria y las caches de los ficheros. El administrador de caches no se limita a gestionar unos cuantos buffers de tamaño fijo para cada fichero abierto, sino que es capaz de estudiar las estadísticas sobre la carga del sistema y variar dinámicamente esos tamaños de acuerdo con la carga. El VMM realiza algo parecido en su trabajo.

- El monitor de referencias a seguridad.

Este componente da soporte en modo privilegiado al subsistema de seguridad, con el que interacciona. Su misión es actuar de alguna manera como supervisor de accesos, ya que comprueba si un proceso determinado tiene permisos para acceder a un objeto determinado, y monitoriza sus acciones sobre dicho objeto. De esta manera es capaz de generar los mensajes de auditorías. Soporta las validaciones de acceso que realiza el subsistema de seguridad local.

- El núcleo (Kernel).

Situado en el corazón de Windows NT, se trata de un micro-kernel que se encarga de las funciones más básicas de todo el sistema operativo: ejecución de subprocesos, sincronización multiprocesador, manejo de las interrupciones hardware.

- El nivel de abstracción de hardware (HAL).

Es una capa de software incluida en el Executive que sirve de interfaz entre los distintos drivers de dispositivo y el resto del sistema operativo. Con el HAL, los dispositivos se presentan al S.O. como un conjunto homogéneo con el cual interacciona a través de un conjunto de funciones bien definidas. Estas funciones son llamadas tanto desde el S.O. como desde los propios drivers. Permite a los drivers de dispositivo adaptarse a distintas arquitecturas de E/S sin tener que ser modificados en gran medida. Además oculta los detalles hardware que conlleva el multiprocesamiento simétrico de los niveles superiores del S.O.

- Llamadas a procedimientos locales y remotos.

Windows NT, al tener una arquitectura cliente-servidor, implementa el mecanismo de llamada a procedimiento remoto (RPC) como medio de comunicación entre procesos clientes y servidores, situados ambos en máquinas distintas de la misma red. Para clientes y servidores dentro de la misma máquina, la RPC toma la forma de llamada a procedimiento local (LPC).

- Llamada a Procedimiento Remoto (Remote Procedure Call -RPC).

Se puede decir que el sueño de los diseñadores de Windows NT es que algún día se convierta en un sistema distribuido puro, es decir, que cualquiera de sus componentes pueda residir en máquinas distintas, siendo el kernel en cada máquina el coordinador general de mensajes entre los distintos componentes. En la última versión de Windows NT esto no es aún posible. No obstante, el mecanismo de RPC permite a un proceso cliente acceder a una función situada en el espacio virtual de direcciones de otro proceso servidor situado en otra máquina de una manera totalmente transparente. Vamos a explicar el proceso en conjunto.

Suponiendo se tiene un proceso cliente ejecutándose bajo una máquina A, y un proceso servidor bajo una máquina B. El cliente llama a una función *f* de una biblioteca determinada. El código de *f* en su biblioteca es una versión especial del código real; el código real reside en el espacio de direcciones del servidor. Esa versión especial de la función *f* que posee el cliente se denomina proxy. El código proxy lo único que hace es recoger los parámetros de la llamada a *f*, construye con ellos un mensaje, y pasa dicho mensaje al Executive. El Executive analiza el mensaje, determina que va destinado a la máquina B, y se lo envía a través del interfaz de transporte. El Executive de la máquina B recibe el mensaje, determina a qué servidor va dirigido, y llama a un código especial de dicho servidor, denominado stub, al cual le pasa el mensaje. El stub desempaqueta el mensaje y llama a la función *f* con los parámetros adecuados, ya en el contexto del proceso servidor. Cuando *f* retorna, devuelve el control al código stub, que empaqueta todos los parámetros de salida (si los hay), forma así un mensaje y se lo pasa al Executive. Ahora se repite el proceso inverso; el Executive de B envía el mensaje al Executive de A, y este reenvía el mensaje al Proxy. El Proxy desempaqueta el mensaje y devuelve al cliente los parámetros de retorno de *f*. Por tanto, para el cliente todo el mecanismo ha sido transparente. Ha hecho una llamada a *f*, y ha obtenido unos resultados; ni siquiera tiene que saber si el código real de *f* está en su biblioteca o en una máquina situada tres plantas más abajo, esta es la elegancia de las RPC.

- Llamada a procedimiento local (Local Procedure Call -LPC).

Las LPC se pueden considerar una versión descafeinada de las RPC. Se usan cuando un proceso necesita los servicios de algún subsistema protegido, típicamente Win32.

El proceso cliente tiene un espacio virtual de 4 Gb. Los 2 GB inferiores son para su uso (excepto 128 Kb). Los 2 Gb superiores son para uso del sistema.

Suponiendo que el cliente realiza una llamada a la función `CreateWindow`. Dicha función crea un objeto ventana y devuelve un descriptor al mismo. No es gestionada directamente por el Executive, sino por el subsistema Win32 (con algo de colaboración por parte del Executive, por supuesto; por ejemplo, para crear el objeto). El subsistema Win32 va guardando en su propio espacio de direcciones una lista con todos los objetos ventana que le van pidiendo los procesos. Por consiguiente, los procesos no tienen acceso a la memoria donde están los objetos; simplemente obtienen un descriptor para trabajar con ellos.

Cuando el cliente llama a `CreateWindow`, se salta al código de esa función que reside en la biblioteca `USER32.DLL` asignada en el espacio de direcciones del cliente. Por supuesto, ese no es el código real, sino el proxy. El proxy empaqueta los parámetros de la llamada, los coloca en una zona de memoria compartida entre el cliente y Win32, pone al cliente a dormir y ejecuta una LPC. La facilidad de llamada a procedimiento local del Executive captura esa llamada, y en el subsistema Win32 se crea un subproceso que va a atender a la petición del cliente.

Ese subproceso es entonces despertado, y comienza a ejecutar el correspondiente código de stub. Los códigos de stub de los subsistemas se encuentran en los 2 Gb superiores (los reservados) del espacio virtual del proceso cliente. El stub correspondiente desempaqueta los parámetros del área de memoria compartida y se los pasa a la función `CreateWindow` situada en el espacio de Win32. Ése sí es el código real de la función.

Cuando la función retorna, el stub continúa, coloca el descriptor a la ventana en la memoria compartida, y devuelve el control de la LPC al Executive. El subproceso del Win32 es puesto a dormir. El Executive despierta al subproceso cliente, que estaba ejecutando código proxy. El resto de ese código lo que hace es simplemente tomar el descriptor y devolverlo como resultado de la función `CreateWindow`.

CAPITULO 10 ADMINISTRACION Y CONFIGURACION DE REDES LOCALES EN WINDOWS 2000

En este capítulo hablo principalmente de las ventajas y diferencias del Windows 2000 con respecto a los sistemas operativos que hablamos en los capítulos anteriores, así como es su configuración.

10.1.- ¿COMO ES WINDOWS 2000?

Windows 2000 representa un esfuerzo por unificar lo que hasta ahora eran dos sistemas operativos distintos, Windows 9x y Windows NT. Desde hace dos años se sabía que Windows NT 5.0 estaba en proyecto, pero Windows 2000 llegó a resolver de una vez por todas las dudas: es la nueva versión de Windows NT 4.0 Workstation y NT Server, pero también incorpora la sencillez de manejo de la serie 9x. Dicho en otras palabras, Windows 2000 ofrece lo mejor de ambos mundos: la solidez y la seguridad de NT, junto a la facilidad de manejo, soporte de hardware y multimedia de Windows 98.

Entre lo mejor de Windows 98 que ofrece la versión 2000, se encuentra el soporte de hardware, la interfase –renovada, incluso-, la presencia de Internet Explorer 5 y del Reproductor de medios, y soporte para las nuevas tecnologías como USB, FAT32, Administración Avanzada de Energía, etc.

10.2.- ¿CUALES SON ALGUNAS DE LAS MEJORAS DE ESTA VERSIÓN DE WINDOWS?

Después de una exploración veloz, se pueden señalar grandes rasgos del nuevo sistema operativo: abundancia de herramientas de conectividad, madurez de la interfaz, buen reconocimiento del hardware y estabilidad. Se añade a esto el soporte de nuevas tecnologías, las mejoras en sus funciones de informática remota, aplicaciones centralizadas de servicio y reinicios obligatorios drásticamente reducidos. Muchas de las mejoras en W2000 son sutiles, pero en conjunto crean una mejor experiencia en el uso de un ordenador. Lo cierto es que después de trabajar unas semanas con Windows 2000, no se echa de menos W98.

10.3.- ¿EN QUE VERSIONES VIENE WINDOWS 2000?

La familia Windows 2000 está integrada por cuatro versiones:

- Windows 2000 Professional: Windows 2000 Pro, sucesor de NT Workstation, está destinado a ser un cliente de red seguro y una estación de trabajo corporativa. Soporta hasta 2 procesadores y es útil, como sistema operativo autónomo, para correr aplicaciones de alta performance, especialmente en diseño gráfico, por ejemplo. Microsoft lo promociona como el principal sistema operativo de escritorio en un entorno de negocios.

- Windows 2000 Server: sucesor de NT Server, soporta hasta 4 procesadores y está destinado a ser el servidor de impresión, archivos, aplicaciones e, incluso, Web de una empresa pequeña a mediana.
- Windows 2000 Advanced Server: sucesor de NT Server Enterprise Edition, soporta hasta 8 procesadores y será el servidor departamental de aplicaciones en empresas medianas a grandes, con más de un dominio y tareas de misión crítica. Entre otras prestaciones, se incluye soporte para RAID y fault tolerance.
- Windows 2000 Data Center Server: soporta hasta 32 procesadores y sólo se entregará sobre pedido. Está destinado a grandes empresas que requieran data warehousing, análisis econométricos, simulaciones científicas e ingenieriles a gran escala, etc.

10.4.- ¿CUALES SON LOS REQUISITOS DE HARDWARE?

No hay que ser modesto con Windows 2000. Los requerimientos mínimos para Windows 2000 Professional son, en el papel, un Pentium 166 MHz, 64 Mb de RAM y 2Gb de disco duro, con espacio libre de, al menos, 1 GB. Esto son números para que el sistema W2000 Professional pueda funcionar. Las versiones Server y Advanced Server requieren procesadores más potentes y más RAM (al menos 256 Mb). En resumen, se recomienda que si deseas instalar W2000 y obtener un nivel aceptable de rendimiento (sobre todo para las versiones Server) optes por una máquina Pentium III 500 Mhz con 256 Mb de RAM como mínimo.

10.5.- ¿COMO ES LA INSTALACIÓN?

La instalación de WIN 2000 Pro puede realizarse sobre W98, aunque las versiones Server y Advanced Server requieren NT o una instalación limpia. El proceso empieza simplemente ejecutando el archivo Setup. Tras unos breves cuadros de opciones para la selección del lenguaje y de accesibilidad, se procede a la copia de archivos de instalación en el disco duro. Previamente, el asistente advertirá si uno desea convertir el sistema de archivos FAT o FAT32 a NTFS. Se recomienda hacerlo, ya que este sistema permite utilizar más eficientemente las funciones de administración de archivos. Una vez terminado, el sistema se reinicia automáticamente y empieza la instalación. El proceso de instalación es largo, pero no necesita demasiada atención y es capaz de aplicar el reconocimiento plug-and-play de forma óptima.

La versión comercial de Windows 2000 es capaz de reconocer y dar soporte a multitud de dispositivos, asignando de forma automática los recursos e instalando los controladores. El nuevo Asistente para la instalación de hardware permite añadir, configurar, quitar, resolver conflictos y actualizar los periféricos de forma dinámica sin preocuparse sobre los efectos en el resto del sistema. De cualquier forma, aunque el soporte de hardware con BIOS antiguas está contemplado, las ventajas mayores se conseguirán sin duda con hardware nuevo, bien USB, AGP OpenGL 1.2 o DirectX.

El reconocimiento del hardware es la parte más larga de la instalación. Una vez terminada la copia de archivos y controladores, el sistema se reiniciará y entremos en la fase de configuración, creación, creación de accesos y registro de componentes. La primera vez que se arranca Windows 2000 notaremos que demora algo más que W98. En la versión Server y superiores, el administrador de red tiene la opción de realizar la instalación de W2000 de forma remota sobre las máquinas cliente.

10.6.- ¿QUE TIPO DE SOPORTE DE HARDWARE PRESENTA WINDOWS 2000?

En lo que se refiere a soporte de hardware, las dos tecnologías que componen los cimientos de Windows 2000 son Plug and Play y ACPI (advanced Configuration and Power Interface), ambas en la base del soporte de hardware de Windows 98. En términos de Microsoft, el conjunto de ACPI y Plug and Play se conocen como la Iniciativa OnNow.

Esta iniciativa de diseño hace que las computadoras estén inmediatamente disponibles. En otras palabras, sin OnNow, las PC's bootan cuando se las enciende. Con OnNow, éstas pasan de un estado de bajo consumo de energía directamente al estado de funcionamiento, y viceversa. Cuando una computadora no está en uso, permanece en un estado en el que parece apagada; sin embargo, todavía está en condiciones de reaccionar a los eventos que se puedan producir en su entorno. En términos comunes, OnNow permite la suspensión y la hibernación. En este último caso, el sistema operativo vuelca en un archivo del disco rígido el contenido de la memoria y se apaga. Al reiniciarse, vuelve a invocar el archivo de la memoria y el Escritorio aparece exactamente igual que antes de apagarse.

Windows asume el control de la configuración del sistema y de la administración de la energía a través de los BIOS Plug and Play y APM (Advanced Power Management). Para esto usa un modelo unificado de controladores –unificado porque sirven tanto para Windows 98 como para 2000-llamado Windows Driver Model (WDM), que soporta Plug and Play y administración de energía para el dispositivo que controla.

10.7.- ¿QUE CAMBIOS GRÁFICOS APARECEN?

Nuevos íconos de sistema y una visualización aparentemente más tridimensional es lo primero que llama la atención. Sobresale, por ejemplo, la posibilidad de que el puntero del Mouse aparezca con una sombra por detrás, que ki destaca del fondo.

10.8.- ¿QUE NOVEDADES HAY RESPECTO A LA INTERFAZ?

Las sorpresas de W2000 empiezan con el menú Inicio. Se diferencia en algo fundamental con relación a versiones anteriores: es capaz de hacer seguimiento de los programas y archivos que se utilizan durante las primeras sesiones. El sistema utiliza este perfil de comportamiento para configurar el menú Programas, de forma que siempre aparezcan las aplicaciones más utilizadas en primer plano, mientras que las restantes se encuentran "recogidas" en el menú. Esto no sólo facilita el acceso a los programas, sino que da una mayor limpieza visual en pantalla. Además, es posible poner en cascada el panel de control y activar el despliegue suave de los menús, con un efecto fado tranquilizador

Entre los detalles más interesantes de W2000 destaca la nueva estructura de los cuadros de diálogo Abrir, Imprimir o Guardar. Estos cuadros presentan un diseño tipo Outlook que permite el acceso rápido a los archivos más utilizados. Además de la carpeta Mis Documentos, tenemos al alcance otras denominadas Mis Imágenes (donde se guardan por defecto los archivos gráficos) y Mis Sitios (donde se han centralizado todos los recursos de red). La barra de navegación de los cuadros de diálogo incluye también una lista de los documentos utilizados recientemente.

10.9.- ¿QUE FACILIDADES DE USO PRESENTA EN SU INTERFAZ?

La personalización y configuración del sistema se puede realizar casi por completo desde los paneles de control, incluyendo las opciones de carpetas. Windows 2000 es el primer sistema operativo que permite personalizar la barra de menús del sistema. De hecho, dispondremos de más de 20 botones incluyendo el de Búsquedas, Mover a, Copiar a, Favoritos y redimensionamiento. Un detalle que los que empiezan con Windows apreciarían es que se han integrado las etiquetas de ayuda contextual a todos los elementos del sistema y que los cuadros de diálogo y paneles son más informativos, incluyendo botones para la resolución de problemas y la opción de desinstalar controladores.

El verdadero trabajo se nota en el Explorador de Windows y la integración con Internet Explorer 5. El Historial de IE5 y del Explorador de Windows incluye ahora tanto los sitios Web como los documentos y carpetas con los que trabajamos y se puede decir que podemos utilizar indistintamente tanto uno como otro para movernos por el sistema.

Los cambios en la herramienta de búsqueda guardan grandes similitudes con las que podemos encontrar en un portal de Internet, ya que acepta operadores voléanos, permite acotar las zonas (en Internet, Archivos y carpetas, o Personas) y especificar al detalle los atributos del requerimiento. Los documentos encontrados se previsualizan en la ventana del Explorador, y a través de esta también podemos acceder a sitios Web o navegar por el disco, una unificación de funciones que parecerá natural a los pocos minutos. Una búsqueda a fondo requiere la ejecución de Index Server. Este componente proporciona la indexación del contenido local en modo subordinado. El usuario puede seleccionar los directorios que quiere indexar y las propiedades que deberían tenerse en cuenta en este proceso. Si el usuario está en una red W2000 Server, el servidor puede hacerse cargo de todo el trabajo.

10.10.- ¿EXISTEN LAS "PANTALLAS AZULES" EN ESTA VERSIÓN?

Windows 2000 es posiblemente el sistema más fiable que haya salido de la casa Microsoft. Las famosas "pantallas azules" que aparecían en momentos críticos de las tareas del servidor se han convertido en una especie extinguida. Esto se ha logrado mediante un conjunto de tecnologías como la protección de escritura del modo kernel; y la "pool tagging", una técnica que permite que los controladores utilicen memoria asignada de un segmento especial y no de la memoria compartida del sistema. Un método de firma digital encriptada se usa para comprobar la fuente e idoneidad del controlador. Si W2000 detecta que un controlador procede de una fuente no certificada avisa al usuario y le da la opción de detener o continuar.

También se ha reducido al mínimo el número de veces que había que reiniciar la máquina cada vez que se cambiaban las configuraciones del sistema. Los más de 75 casos en los que el reinicio era condición indispensable se han reducido a siete. Mejor aun, W2000 incluye algunos mecanismos que previenen las inestabilidades antes de que lleguen a suceder. El Servicio de instalación contribuye a ello gestionando los componentes compartidos, una de las fuentes de conflicto más frecuentes de W95 y W98. El instalador comprueba la integridad de los componentes compartidos, incluso en el caso de que una de las aplicaciones que haga uso de ellos se desinstale.

10.11.- ¿ES FIABLE ÉSTE SISTEMA?

La fiabilidad y la capacidad de gestión se han mejorado con herramientas que ayudaran a los usuarios y administradores de red a gestionar de forma más sencilla sus sistemas, empezando porque el laberinto de las DLLs parece resuelto. Windows 2000 permite que las DLLs (Dynamic Link Libraries) se instalen en los directorios de sus aplicaciones específicas, y eviten que se eliminen las DLLs compartidas.

10.12.- ¿COMO SE LLEVA A CABO LA GESTIÓN DE ESTE SISTEMA?

La gestión global de un sistema se realiza a través de un módulo denominado Administración del equipo, que organiza los recursos, servicios, dispositivos de almacenamiento y seguridad que utilizan tanto en el sistema local como en ordenadores remotos. El panel es una herramienta muy valiosa para los administradores de red y se divide en tres módulos: Herramientas del Sistema, Almacenamiento y Servicios y Aplicaciones.

En Herramientas del Sistema, por ejemplo, disponemos de un visor de sucesos y del Administrador de dispositivos, una síntesis jerarquizada de los dispositivos instalados en el PC y que permite hacer modificaciones y búsquedas para resolver conflictos IRQ o DMA. Por otro lado, desde Almacenamiento es posible acceder a las propiedades de las unidades de disco, incluyendo unidades extraíbles, y a sus opciones de verificación, comparaciones y copias de seguridad. Finalmente Servicios y Aplicaciones nos dan información más clara sobre los servicios Microsoft y de red implementados. En general, el Administrador del equipo es un mapa completo y detallado de la PC, incluyendo informes sobre la forma en que el usuario lo utiliza.

10.13.- ¿QUE INFRAESTRUCTURA DE SEGURIDAD PRESENTA?

Puesto que se trata de un sistema operativo orientado al trabajo en red y a la compartición de recursos, la familia Windows 2000 ha integrado sólidas tecnologías de seguridad. La intención es que cada usuario pueda comprender como funcionan estas tecnologías y controlarlas de forma cabal. Esta "infraestructura" de seguridad funciona en tres niveles:

1. Local. Se refiere a la protección de datos en el ordenador. El sistema esta diseñado para evitar que usuarios no autorizados se "salten" el sistema de arranque y, por tanto, también las funciones de seguridad. Algunos fabricantes de hardware integran sistemas de "contraseña", una solución no muy adecuada para entornos de trabajo compartido. La encriptación de los datos en el disco NTFS es un servicio que se basa en la arquitectura CriptoAPI de Windows para implementar el sistema de llaves públicas. Cada archivo (incluyendo sus temporales de trabajo) se encripta a través de una llave generada aleatoria mente, utilizando algoritmos asimétricos. W2000 es el primer operativo que implementa encriptación de 128 bits en un proceso transparente, ya que ENF encripta y desencripta los archivos localizando las llaves del usuario, bien desde el almacen del sistema o desde los dispositivos como los Smart Cards.
2. Corporativo. Se refiere a la proteccion de datos en una red local. W2000 utiliza el protocolo de autenticación Kerberos versión, 5, un estándar de seguridad en redes locales e intranets que verifica y hace un seguimiento de la actividad de cada usuario dentro de la red. Kerberos permite un control del acceso unificado a casi cualquier entorno de red, eliminando la necesidad de obtener permisos y esperar la respuesta de cada vez que un cliente desea acceder a un nuevo recurso de la red.
3. Publico. W2000 utiliza también sistemas de llaves públicas y protocolos de autenticación para mantener la seguridad de las comunicaciones que se realizan por Internet, de forma que verifique la procedencia de mensajes de correo o garantice las fuentes de donde proceden las descargas. Por otra parte, incluye soporte para redes privadas virtuales (VPN), protocolos encapsulados que crean un "canal" de comunicación privado a través de redes públicas. El soporte VPN se realiza a través del protocolo PPTP (Point to Point Tunneling Protocol), Layer 2 Tunneling Protocol e IPSec, un protocolo que implementa una gama de funciones sobre una capa de red encriptada.

10.14.. ¿QUE ES ACTIVE DIRECTORY?

Un servicio de directorios es un servicio de red que identifica todos los recursos en ella y los vuelve accesibles a los usuarios y a las aplicaciones. Active Directory (AD) es el servicio de directorio incluido en W2000.

El elemento principal de AD es el directorio, que almacena información sobre los recursos de la red y los servicios que hacen disponible la información. Los recursos almacenados en el directorio, como los datos del usuario, impresoras, servidores, bases de datos, grupos, computadoras y políticas de sistema, se denominan objetos.

AD los organiza jerárquicamente en dominios. Un dominio (Domain) es una agrupación lógica de servidores y otros recursos de red bajo un mismo nombre de dominio.

Cada dominio incluye uno o mas controladores de dominio (domain controllers), que son maquinas que almacenan una replica de un directorio de dominio. Cada vez que se hace algún cambio en alguno de los controladores, el resto se actualiza automáticamente.

Un objeto es un conjunto de atributos particulares, bajo un nombre específico, que representa un recurso individual de la red. Los atributos se refieren a las características del objeto. Así, los atributos de una cuenta de usuario pueden ser el nombre, departamento y dirección de mail, y los de una impresora, si es láser y si es en color. Algunos objetos funcionan también como contenedores: por ejemplo, un dominio.

Las agrupaciones lógicas de objetos son las clases. Una clase puede estar constituida por todas las cuentas de usuario, las impresoras, los grupos, etc.

Las unidades organizacionales (UO, organizational units) son contenedores que se usan para reunir objetos de un dominio en grupos administrativos lógicos. Cada UO puede contener distintos objetos y cada dominio puede tener su propia lógica de agrupación en UOs.

La unidad central de la estructura lógica de AD es el dominio. Agrupando los objetos en uno o más dominios es posible representar la propia organización de la empresa. Todos los objetos de la red existen en un dominio, es posible albergar hasta 10 millones de objetos.

Quizás al usuario final este tipo de estructura no le diga nada. Sin embargo, para administrar una red empresarial, AD permite hacerlo de manera fácil, centralizada y automática en muchos de sus parámetros. Y para el usuario significa no tener que recordar números o nombres abstractos, y tener los recursos de la red disponibles sin tener que preocuparse por saber donde están.

10.15.- ¿SE PUEDE USAR WINDOWS 2000 EN COMPUTADORAS PORTATILES?

Aunque W2000 es aparentemente un sistema operativo de gran tamaño, Microsoft ha hecho un gran esfuerzo para que los usuarios de ordenadores portátiles puedan llevarlo en sus maquinas y trabajar con el independiente y coordinadamente a la vez. Para esto, W2000 tiene la capacidad de definir carpetas para el trabajo "off-line". Configurando esta opción es posible trabajar con los documentos en el portátil, con la seguridad de que cuando se realice una conexión con nuestro ordenador principal se realizara la sincronización de todos los archivos. Asimismo, si utilizamos archivos compartidos, cuando se establezca una conexión con la red, obtendremos la ultima versión de aquellos, listos para empezar a trabajar.

La función de ahorro de energía, básica para los usuarios de portátiles, se realiza a través del soporte ACPI. ACPI, también, permite la mejora de la conexión de los portátiles a los docks de los sistemas principales, ya que puede hacerse en actividad y sin retrasos en el reconocimiento del hardware y controladores.

El usuario puede crear también diferentes perfiles de utilización en caso de baja energía, bien disminuyendo el trabajo de disco, el brillo de la pantalla u optando por el modo reposo. W2000 también soporta la "hibernación" de portátiles. La única mala noticia, es que ACPI forma parte del firmware de un sistema, por lo que solo los portátiles de nueva fabricación pueden hacer uso de este estándar.

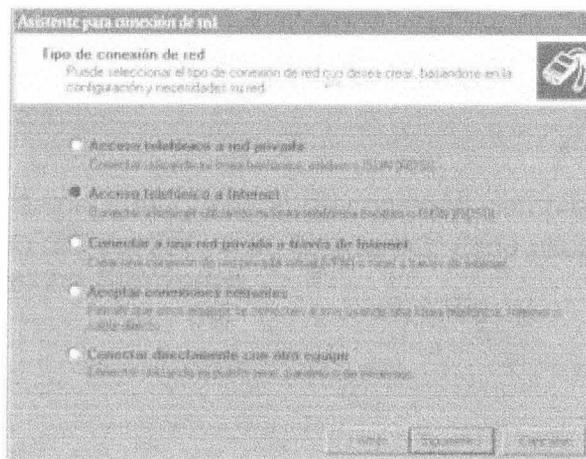
10.16. – CONFIGURACIÓN DEL ACCESO A INTERNET EN WINDOWS 2000

Se recomienda seguir los pasos en orden para instalar satisfactoriamente el acceso a Internet.

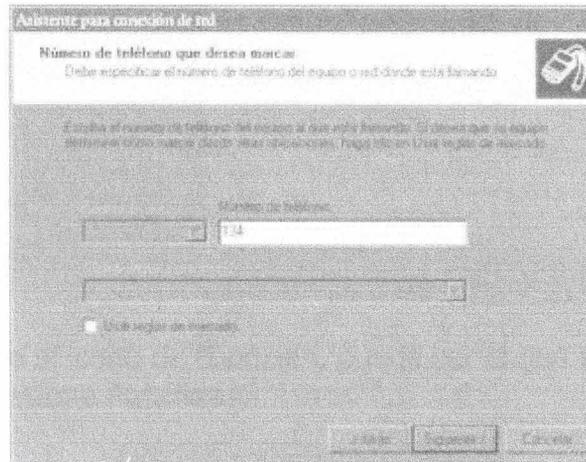
1. Presione el botón **Inicio**, diríjase a: Configuración-->Conexión de Red y Acceso Telefónico-->Realizar conexión nueva.



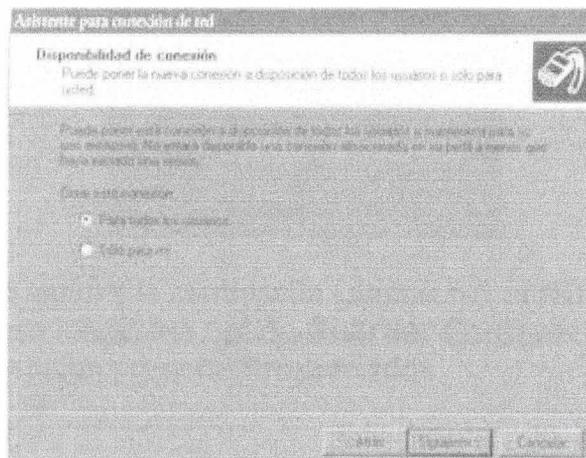
2. Este es el asistente de conexión que le guiará paso a paso para realizar el icono de acceso a Internet.



3. Para conectarse vía MODEM/línea telefónica debe de marcar la segunda opción. Luego presione **Siguiente**.



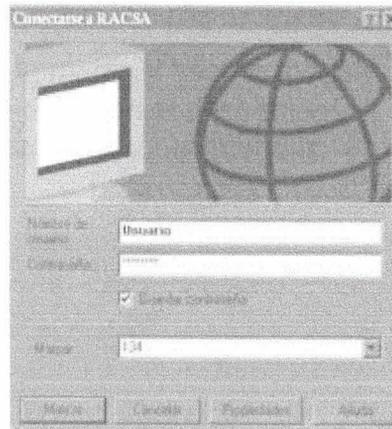
4. Se debe digitar el número telefónico de acceso 134. Además puede utilizar alguno de los números de siete dígitos. Presione **Siguiente**.



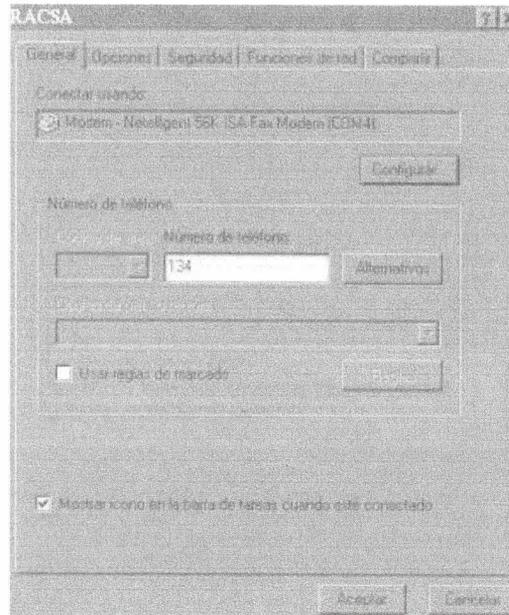
5. Puede manejar una sola configuración de conexión siempre y cuando el equipo **NO** sea de uso compartido, si es compartido cada usuario debe de tener un perfil distinto. Presione **Siguiente**.



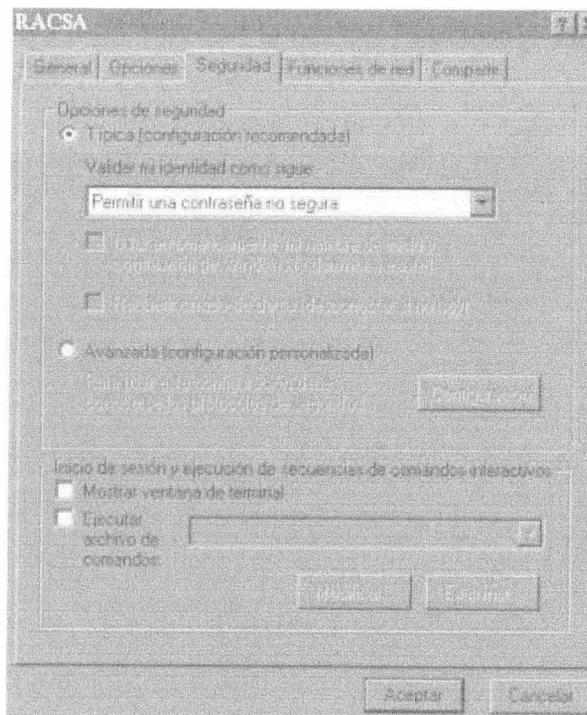
6. Asigne un nombre al icono de conexión, puede ser el que usted decida. Por ejemplo **RACSA**. Presione **Finalizar**.



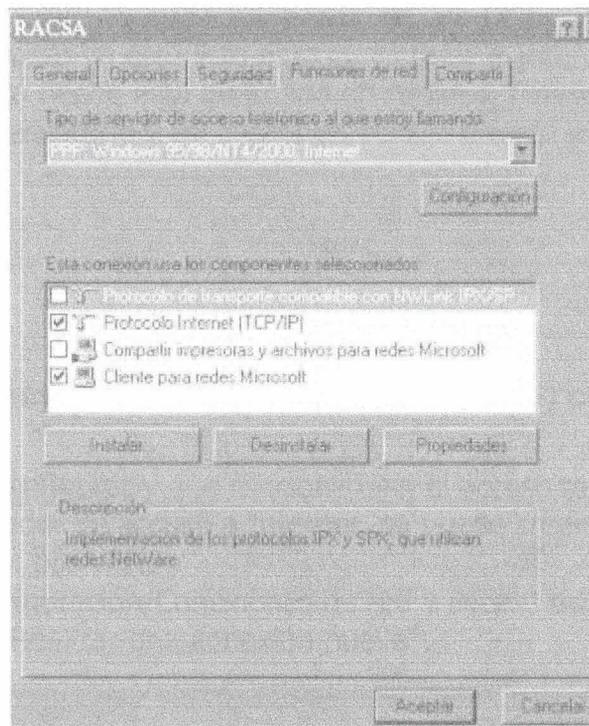
7. Digite su usuario (*login*) y la contraseña (*password*), si **NO** quiere volver a pasar por este proceso marque la opción **Guardar Contraseña**, digite el número de acceso, y luego presione **Propiedades**.



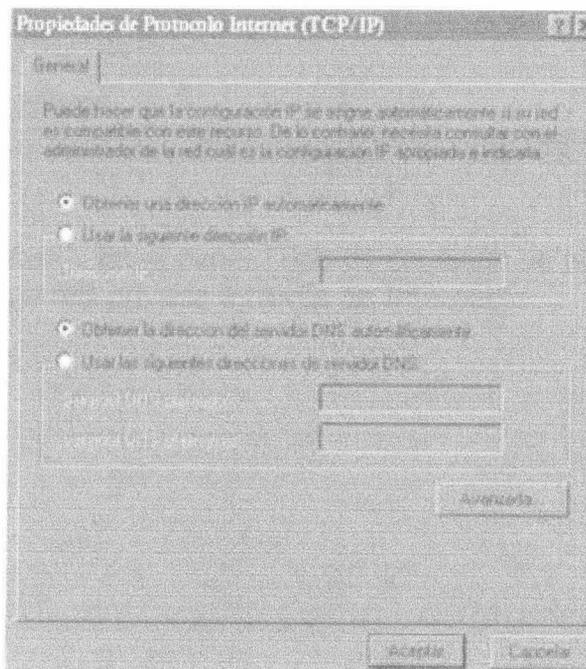
8. Esta pantalla le describe la marca y tipo de módem que tiene el usuario, más el número de acceso que le digito en el paso anterior, marque la opción **Mostrar icono de la barra de tareas**. Presione **Aceptar**.



9. Dejar la marca que tiene la opción de seguridad, ya que es la típica configuración para su buen funcionamiento.



10. En esta pantalla **SOLO** deben estar marcadas estas dos opciones que aparecen, ninguna otra más. Marque la opción **Protocolo Internet (TCP/IP)**, y presione Propiedades.

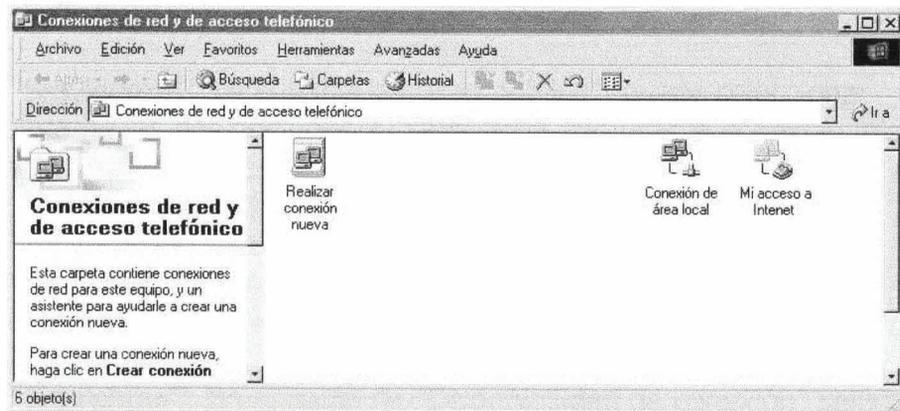


11. En esta pantalla **NO** se debe de cambiar ninguna opción ya que **NO** es necesario especificar *Dirección IP* ni los *Servidores de Nombres (DNS)*.

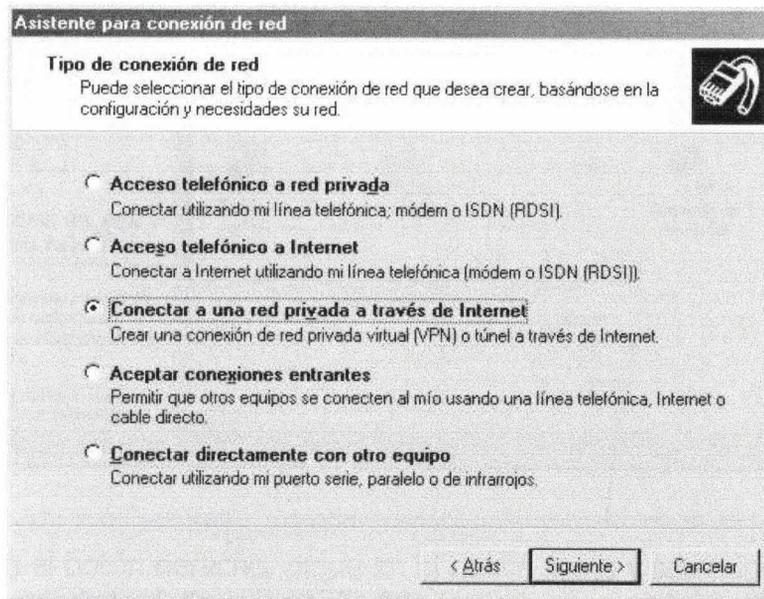
Después de este proceso ya esta listo para conectarse a Internet, recuerde que este icono que hemos hecho esta guardado en **Acceso Telefónico a Redes**, puede arrastrarlo al escritorio y así creara un acceso directo y ejecutarlo desde ahí mismo.

10.17.- Acceso remoto por VPN (Red privada virtual) con Win 2000

1. Después de configurar y que funcione bien el acceso telefónico a redes con un proveedor de acceso a Internet, se puede crear una conexión de acceso remoto por VPN:
2. En Inicio/Configuración/Conexiones de red y acceso telefónico, pulsa en el asistente de "Realizar una conexión nueva":



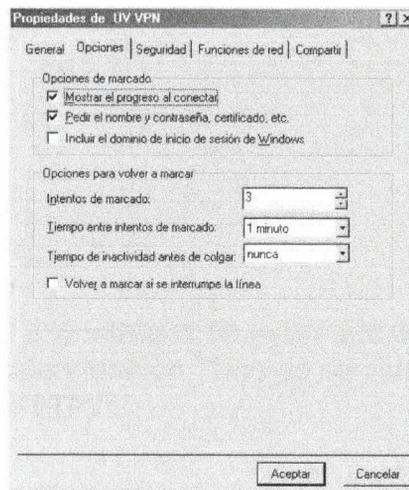
3. Pulse "Siguiente>". En el panel "Tipo de conexión de red", seleccione "Conectar a una red privada a través de Internet":



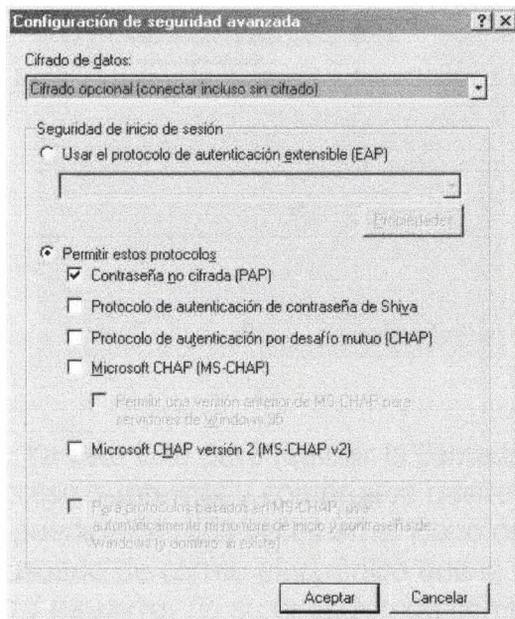
4. Pulse "Siguiete >". En el panel de "Red pública", puede seleccionar cualquiera de las dos opciones. Si selecciona "No usar la conexión inicial", deberá conectarse antes de ejecutar la conexión VPN a su proveedor de acceso Internet. Si selecciona "Usar automáticamente esta conexión inicial", la conexión a Internet seleccionada se establecerá automáticamente antes de lanzar la conexión VPN.
5. Pulse "Siguiete >". En el panel "Dirección de destino", ponga "vpn.uv.mx" como nombre de host:
6. Pulse "Siguiete >". En el panel de "Disponibilidad de conexión" seleccione si quiere que la nueva conexión pueda usarse por todos los usuarios de su ordenador o sólo por UD.
7. Pulse "Siguiete >". Ponga el nombre de la conexión que desee en el último panel, por ejemplo, UV VPN y pulse "Finalizar"
8. Con ello le habrá aparecido el icono de la nueva conexión en la ventana de "Conexiones de red":



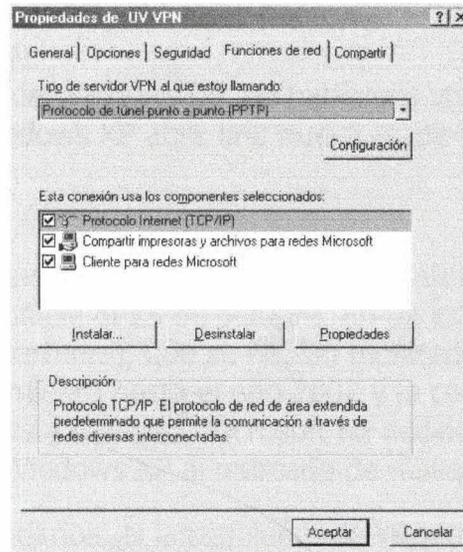
9. Con el botón derecho, pique en el nuevo icono y seleccione "Propiedades". En la pestaña "Opciones", marque la casilla de "Pedir nombre y contraseña, certificado, etc.":



10. En la pestaña de "Seguridad", seleccione "Avanzada (configuración personalizada)", y pulse en el botón de "Configuración". En "Cifrado de datos" seleccione "Cifrado opcional (conectar incluso sin cifrado)". Marque únicamente la opción de "Permitir estos protocolos" y "Contraseña no cifrada (PAP)":



11. Pulse "Aceptar" y "Si" a la ventana de aviso que aparece. En la pestaña de "Funciones de red", seleccione en "Tipo de servidor VPN" "Protocolo de túnel punto a punto (PPTP)":



12. Pulse "Aceptar". Ya está listo para realizar la llamada. Conéctese a su proveedor de acceso a Internet y compruebe que le funciona el acceso a Internet. Ahora puede picar dos veces en el icono de la nueva conexión VPN. Ponga su usuario de correo electrónico que le suministro el administrador (**su usuario**, no su dirección de correo ni ninguna otra cosa) y como contraseña, la que usa para acceder al correo electrónico. Pulse "Conectar":



Se realizará la conexión VPN y a partir de ese momento, estará usando una dirección de la red local que el administrador le proporcione, que le permitirá acceder a los servicios de la misma.

WINDOWS XP Y WHISTLER LAS MEJORAS ESPERADA.

11.1.- INTRODUCCION.

Desde los tiempos de Windows 95, no habíamos visto un cambio tan grande en Windows. Windows XP abre una nueva etapa en los sistemas operativos.

Después de semanas de especulaciones, Microsoft ha anunciado que Windows XP estará disponible el 25 de octubre. En un esfuerzo por aliviar los temores de sus socios (partners), que se habían mostrado inquietos ante un posible retraso del lanzamiento hasta el año 2002 y la consecuente pérdida de la campaña de regalos de esta Navidad, Microsoft ha decidido hacer público su calendario para ofrecer Windows XP al mercado de masas.

«Marquen sus calendarios: el lanzamiento de Windows XP, el 25 de octubre, será un día histórico para nuestros usuarios y para la industria», ha afirmado Steve Ballmer, presidente de Microsoft. «Windows XP será el sistema operativo de mayor calidad que haya elaborado jamás Microsoft, y además tanto Microsoft como nuestros socios nos hemos comprometido a ofrecer una serie de nuevas y sorprendentes posibilidades informáticas que supondrán un nuevo paradigma para los usuarios de PC de todo el mundo». De momento, Microsoft ha confirmado que la inversión en mercadotecnia para promocionar Windows XP será un récord en la historia de la compañía: sólo durante los primeros cuatro meses en que esté disponible el producto, la compañía doblará la cantidad de dinero que se gastó durante el primer año de vida de Windows 95.

11.2.- VERSIONES PRELIMINARES

Antes de presentar la versión final de Windows XP, Microsoft desarrollará una primera versión preliminar (Release Candidate 1 o RC1) que enviará a cientos de miles de clientes, y una segunda versión preliminar (RC2) en la que se prevé introducir muchos menos cambios. La versión RC1 tendrá prácticamente todas las características y funciones de Windows XP, según fuentes de Microsoft, y estará por tanto mucho más cerca de la calidad final del producto que la actual beta 2. La versión RC2 será prácticamente idéntica a la versión final.

11.3.- DOS VERSIONES XP Y UNA VERSION SERVER

Windows XP se venderá en dos versiones: Windows XP Home Edition, destinada al mercado de consumo, y Windows XP Professional Edition, orientada a profesionales. Una versión de 64 bits de Professional Edition, diseñada para el procesador Itanium de Intel, también estará disponible tan pronto Intel comercialice el procesador (las primeras estimaciones apuntan que el Itanium estará disponible este otoño, si bien Intel no ha concretado aún una fecha exacta).

En esta beta 2 ya se vislumbra lo que Microsoft esta preparando, una auténtica revolución, el siguiente paso en la integración del sistema con el usuario y todo ello teniendo Internet como tecnología céntrica.

Un repaso exhaustivo a todas las partes de Windows XP Home beta2, haciendo especial hincapié en las novedades que no son pocas: interface de usuario, administrador de archivos, multimedia, Internet, System Restore, Firewall y nuevo sistema de drivers.

11.4.- NUEVA INTERFAZ.

La nueva interfaz salta a la vista por su nuevo diseño y facilidad de uso. Todo ha sido rediseñado para orientar al usuario en las tareas más comunes dentro del contexto en que se encuentra.

11.5.- PANTALLA DE INICIO Y CAMBIO RÁPIDO DE USUARIOS.

Con Windows XP es fácil compartir el mismo PC entre distintos usuarios, incluso una vez iniciado. La primera pantalla nos muestra la lista de usuarios del PC que se pueden añadir durante la instalación del sistema o desde el panel de control.

Todos los parámetros del sistema son personalizables por usuario. Esto quiere decir que desde la imagen que aparece al lado del nombre, hasta el aspecto visual, favoritos, vistas, etc... se adaptarán a cada usuario. Los usuarios pueden proteger sus cuentas estableciendo contraseñas.

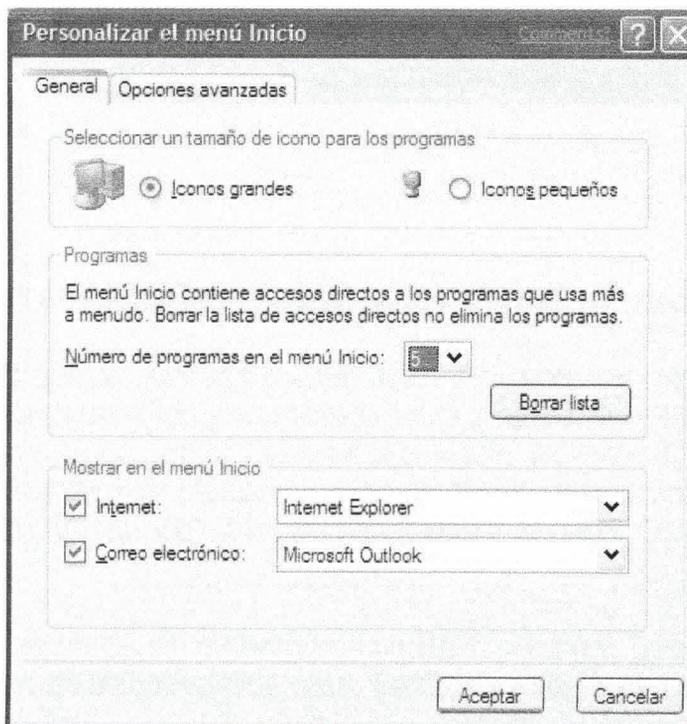
Además, podemos intercambiar de usuario sin que se pierda lo que se está haciendo. Supongamos que Marta está usando el sistema y que Juan quiere comprobar si tiene correo nuevo. Basta que Marta seleccione que desea dejar el PC a Juan para que este empiece a trabajar con el como lo haría normalmente. Mientras tanto, las aplicaciones de Marta siguen ejecutándose mientras Juan usa las suyas. En cualquier momento, Juan puede cederle el control del PC a Marta mientras su correo se descarga.

11.6.- NUEVO MENÚ INICIO Y BARRA DE TAREAS.

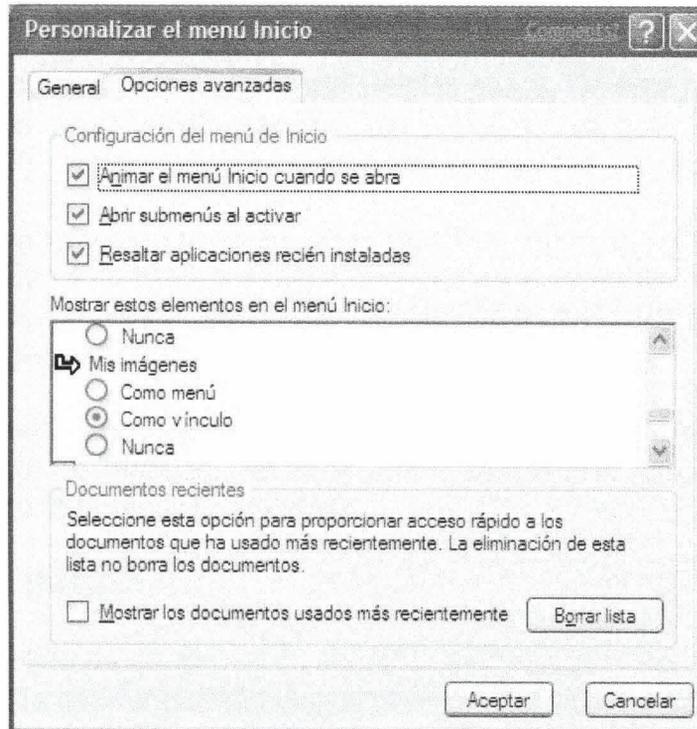
El nuevo menú inicio agrupa las aplicaciones más usadas para que tengas el acceso más fácil a ellas. El usuario ve primero las aplicaciones y encima de estas sus programas de acceso a Internet y de correo electrónico por defecto. Se acabó el buscar una aplicación dentro de las infinitas ramas del menú de inicio clásico. A la derecha, tenemos acceso rápido a las conexiones a Internet, documentos, ayuda, etc.



El nuevo menú inicio y la barra de tareas son totalmente personalizables pudiendo ser desactivado para usar el menú inicio clásico de Windows y personalizado añadiendo y quitando elementos, especificando el número de programas más recientes que deberían ser listados, etc. Destacan dos opciones nuevas, la primera permite agrupar los botones similares. Hasta ahora, teníamos un botón por ventana abierta, XP agrupará los similares teniendo todas las ventanas abiertas de un programa bajo un mismo grupo. Por ejemplo, en la imagen inferior vemos las ventas de Internet Explorer agrupadas.



El área de notificación ha sido también mejorada ocultando aquellos elementos que no estén activos.



11.7.- INTERNET Y MULTIMEDIA LLEVADOS AL MÁXIMO EXPONENTE.

Nos hemos quedado sorprendidos con todas las mejoras multimedia y de internet que hemos ido encontrando en el sistema. Windows XP es definitivamente un primer paso hacia la visión .NET de Microsoft. El énfasis que se hace para permitir compartir archivos, fotos, charlas entre amigos y familia (o con el resto del mundo) hace de Windows XP el mejor OS jamás visto para tales propósitos.

No se olvida sin embargo de aquellas personas que deban conectarse a sus puestos de trabajo desde casa. Escritorio remoto permite controlar el PC de la empresa desde casa con un solo clic. Además, Windows XP permite interconectar PCs de modo fácil para compartir archivos, música o una conexión a Internet.

11.8.- TRABAJANDO CON IMÁGENES.

La carpeta "Mis imágenes" ha sido totalmente rediseñada permitiendo distintas formas de ver las imágenes, publicarlas en Internet o enviarlas por correo electrónico a amigos y familia. Windows XP redimensiona si el usuario lo desea las imágenes que van a ser enviadas/publicadas para que ofrezcan la mejor calidad con el mínimo tamaño lo cual nos facilita la pesada tarea de redimensionar nuestras fotos digitales de 2MB para enviarlas por correo electrónico. Integraciones de comercio electrónico nos permiten pedir copias impresas de nuestras fotos siguiendo simples pasos. De este modo, nos ahorramos tener que grabar un CD y llevarlo a la tienda para que las fotos sean impresas.

Si disponemos de una cámara fotográfica digital, el tema se pone aun más interesante. Con sólo pincharla, Windows XP nos la muestra como elemento en "Mi PC", basta con abrirla para poder ver las imágenes grabadas en la cámara, rotarlas, redimensionarlas, grabarlas a disco, etc.

Para todos los poseedores de impresoras de color, Windows XP dispone de un asistente de impresión de fotografías que nos guía paso a paso en todo lo necesario para la impresión de éstas.

11.9.- MULTIMEDIA.

Multimedia da un paso más adelante integrando el Reproductor de Windows Media con funcionalidades específicas del sistema operativo como son la reproducción de DVDs y la grabación de CDs. La inclusión de código de grabación de CDs hace que sea igual de fácil grabar archivos en un CD como lo es en el disco duro. Podemos mover, copiar y desplazar cualquier archivo a la unidad de CD-R y éste se grabará automáticamente. Igualmente podremos añadir nuevos archivos realizar cualquier tipo de cambios hasta que decidamos cerrar la sesión de grabación. La sesión puede cerrarse en cualquier momento o dejarse abierta mientras lo deseemos. En el último caso, sólo los usuarios de Windows XP podrán leer nuestros CDs. Basta con cerrar la sesión para que el CD-R se convierta en un CD grabado estándar.

El hecho de que el reproductor de Windows Media 8 soporte lectura de DVD y grabación de CD-R provenientes del código del sistema operativo, hace que sea el primer Reproductor de Windows Media que no será publicado en Internet. En otras palabras, sólo los usuarios de Windows XP podrán disfrutar de estas mejoras.

Esta vez, el reproductor va más allá y permite copiar canciones de un CD de música a MP3 ampliando así las posibilidades de la versión 7 que sólo permitía la copia al formato WMA (Windows Media Audio) Esto se ha producido en respuesta a la creciente demanda de usuarios del formato MP3 pidiendo compatibilidad de las canciones grabadas con otros sistemas operativos como Mac y Linux. Recientemente, Microsoft lanzó la versión Mac de Windows Media Player 7. No obstante, para usuarios Windows preocupados por la cantidad de espacio ocupado en el disco por sus canciones MP3, esta versión 8 del reproductor viene con un nuevo codec que ofrece calidad CD a 64kbps, o lo que es lo mismo, calidad superior en la mitad de espacio de un MP3.

Igualmente, WMA ofrece la posibilidad de proteger digitalmente las canciones (solo formato WMA), para aquellos que deseen canciones que puedan ser reproducidas por todos, basta con ir a Herramientas, Opciones y desmarcar la casilla de uso de derechos digitales.

La tecnología de administración de derechos digitales de Microsoft (DRM) aun está a salvo de hackers y es la máxima candidata a salvar a Napster de sus apuros con las discográficas. Entre otras cosas, la tecnología permite escuchar libremente una canción hasta una cierta fecha, y requerir un pago por ella para escuchas posteriores.

Otra mejora sustancial es la inclusión de controles en el modo de visionado en pantalla completa. Los controles aparecen al desplazar el ratón hacia la parte superior de la pantalla.

11.10.- MI MÚSICA.

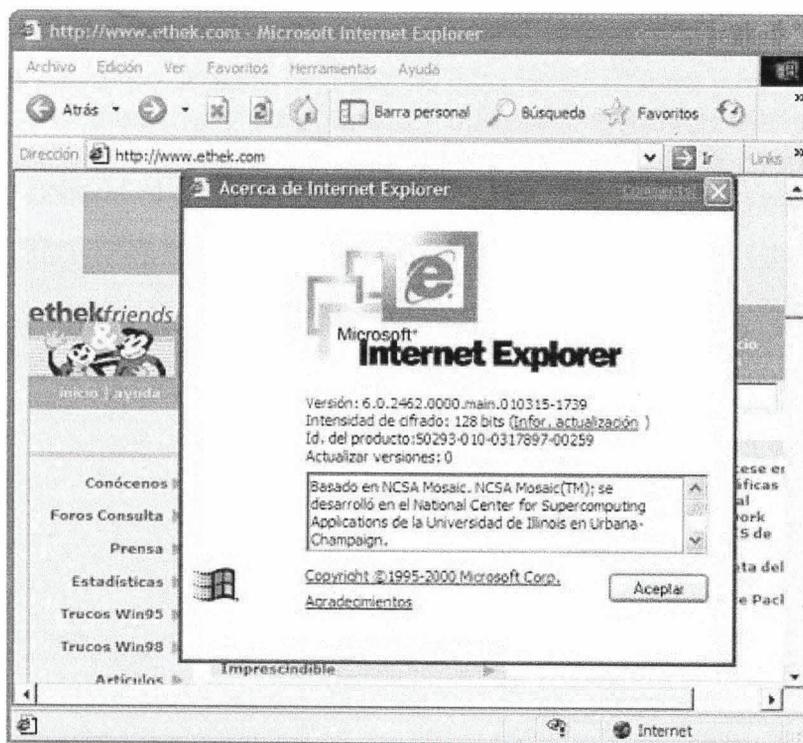
Una colección de Lenny Kravitz organizada automáticamente por álbumes. Las carátulas vienen directamente de Internet y es una de las nuevas funcionalidades del Shell de Windows XP que nos permite cambiar el icono de las carpetas, así como asignar una imagen de alta resolución a las carpetas en vista miniatura. Igualmente, como hemos visto en Mis imágenes, la inclusión de una o más imágenes en una carpeta hará que Windows XP nos muestre un mosaico con las primeras 4 imágenes de la carpeta para que nos sea más fácil encontrar la que buscamos.



Sin perder la visión característica de negocio de Microsoft, la carpeta incluye links que permiten hacer búsquedas de tiendas online para comprar la música del artista seleccionado.

11.11.- INTERNET.

Internet Desde la inclusión de MSN Explorer y Messenger, Microsoft satisface a los usuarios de Hotmail y MSN. Con la integración de un calendario, lista de tareas, información personalizada, MSN Explorer parece la mejor opción para aquellos usuarios con necesidades limitadas y que quieran poder acceder a su información desde cualquier PC o dispositivo. La versiones de Internet Explorer y Outlook Express es la 6.0.



Windows XP y la conexión a Internet El uso de los últimos protocolos en calidad de servicio (QoS) hacen que la conexión a Internet se halla acelerado considerablemente respecto a todas las versiones anteriores Windows con cuotas de compresión de hasta el 70%. Todos los usuarios notarán la diferencia pero especialmente aquellos con conexiones de banda ancha verán incrementos descomunales en su velocidad de conexión, especialmente en el tiempo de que tarda el explorador en conectar a un servidor.

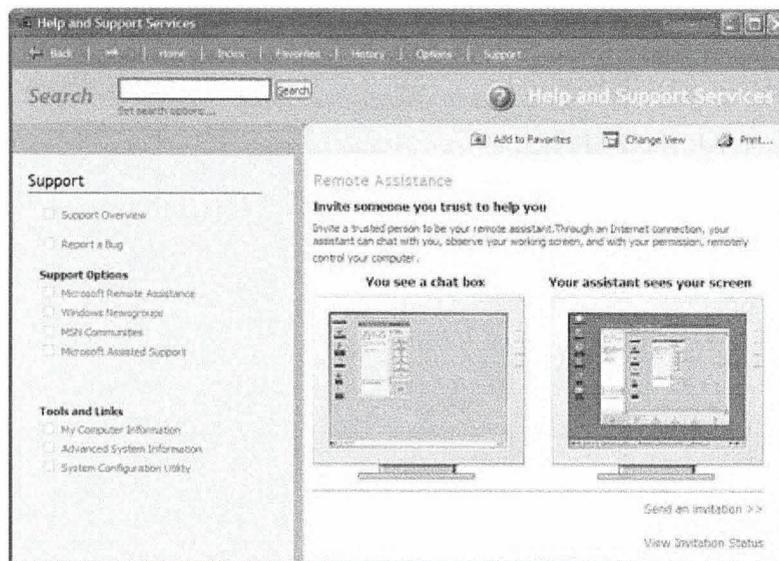
El asistente para compartir conexión a Internet incluye ahora una opción específica para las conexiones de banda ancha, facilitando compartir una conexión ADSL entre distintos PCs del hogar o de una comunidad de vecinos.

11.12.- ROBUSTEZ, SEGURIDAD Y FIABILIDAD.

Basado en el núcleo de Windows 2000, Windows XP es una revolución tecnológica para el usuario doméstico y para cualquier persona que no use Windows 2000 actualmente. Además, Microsoft nos sorprende con las mejoras de mantenimiento del sistema operativo que permiten desde que un amigo te ayude remotamente configurando tu PC, hasta mantener el sistema operativo automáticamente actualizada con las últimas actualizaciones críticas permitiendo al usuario mantener el sistema operativo a la última sin el menor esfuerzo.

11.13.- ASISTENCIA REMOTA.

Hemos realizado simples pruebas de esta funcionalidad y hemos quedado gratamente sorprendidos por su potencia y utilidad. A través de Messenger, por email o simplemente intercambiando un archivo, se puede pedir ayuda a un compañero y cederle el control de nuestro PC para que nos solucione un



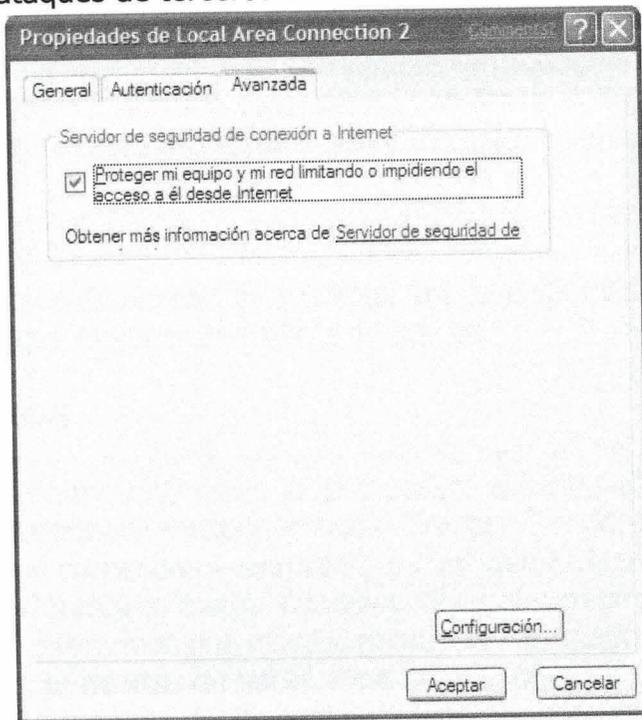
problema. Evidentemente, podemos cortar la comunicación en cualquier momento si el compañero decide hacernos alguna jugada. ¿Cuántas veces le has pedido ayuda a alguien y has tenido que ir anotando paso a paso la manera de hacer lo que querías? Bueno, pues aquí está tu solución, le contactas con Messenger o le mandas un email y listos.

Igualmente, para problemas de mayor gravedad, el servicio de soporte técnico de Microsoft, podrá ayudarte a solucionar un problema sin que tengas que pulsar una sola tecla. Para obtener una seguridad adicional, puedes especificar una contraseña que la persona que vaya a ayudarte deberá introducir para poder ayudarte.

Tu verás una pantalla de chat y la persona que te ayude, verá tu escritorio.

11.14.- CORTAFUEGOS (FIREWALL).

Para proteger tu conexión a Internet, Windows XP incluye un firewall que impide los ataques de terceros desde Internet cuando estás conectado.



11.14.- RESTAURAR SISTEMA.

Al igual que Windows Me, XP ofrece la posibilidad de restaurar el PC a una configuración anterior, permitiendo recuperar el PC tal y como estaba en una fecha determinada, antes de instalar alguna aplicación o hardware dañinos o simplemente tal y como estaba antes de que se lo prestáramos a un amigo patoso.

11.15.- DRIVERS.

Firmados y certificados Antes de comprar un dispositivo deberíamos mirar si éste está certificado para ser usado con Windows. La certificación significa que los drivers del dispositivo cumplen los requisitos de calidad del sistema operativo y que no ponen en peligro su uso. Desde Windows 98 SE, Microsoft ha presentado un nuevo modelo de drivers, llamados Windows Driver Model (WDM) que impiden que los drivers puedan hacerle jugadas al sistema operativo. A menudo los fabricantes prueban sus drivers con sus periféricos y se despreocupan de su interacción con otros dispositivos de otras marcas. Los drivers son los causantes de las famosas pantallas azules y no hay que olvidar que es código escrito por el fabricante del dispositivo y no por el del sistema.

A menudo, los fabricantes usan logos "alternativos" para hacer pensar al usuario que dicho hardware es compatible con todas las versiones de Windows. Para evitar esto, el sistema exige ahora una firma digital en los drivers, que certifica que han sido probados y han pasado los requisitos de calidad mínimos.

Al intentar instalar drivers no certificados, recibimos un aviso a plena pantalla recomendándonos no instalarlos. Evidentemente, somos libres de hacerlo pero es de agradecer que cada vez se exija más abiertamente a los fabricantes que desarrollen drivers de calidad.

CONCLUSIÓN.

En definitiva, Windows XP nos parece el paso definitivo en lo que podríamos llamar sistemas operativos clásicos. Cumple con todas las necesidades de un usuario doméstico y avanzado, y hará que olvidemos viejas glorias fácilmente. Del mismo modo, Windows XP es el primer paso hacia la nueva era de sistemas operativos que revolucionarán la informática con capacidades de reconocimiento de voz, de habla. Con almacenamiento de datos unificado e información disponible desde cualquier lugar y desde cualquier dispositivo.

Siendo sólo una Beta 2 (compilación 2462) y habiendo visto la robustez que tiene, no nos extrañaría que Windows XP nos presentara aun alguna sorpresa en su versión final.

CAPITULO 12

TRUCOS, RECOMENDACIONES Y ALGO MAS DE REDES LOCALES.

12.1 ENCONTRAR UN PC EN LA RED

Si odias ir a través del Entorno de Red para ENCONTRAR UN ORDENADOR EN LA RED u odias buscar a través de Mi PC o el explorador cuando sabes exactamente donde quieres ir, aquí tienes la solución. Haz click en Inicio-> Ejecutar-> y escribe la ruta. Por ejemplo: Inicio-> Ejecutar-> C:\win95> abrirá una ventana del directorio Win95. Entonces haz lo siguiente Inicio-> Ejecutar-> o puedes usar el nombre del servidor solamente. Si estás buscando un ordenador, esto te ayudará a hacerlo más rápido.

12.2.- UNA RED Y UN CD-ROM (CONSEJOS)

En realidad no es un truco, es algo que le puede pasar a cualquier persona : En una LAN, solo una computadora tiene CD-ROM, por lo que intente compartir el CD con el nombre CD, la LAN funcionaba perfecta, yo podía leer, trabajar y ejecutar cosas en el disco duro de la computadora con CD, sin embargo, cuando yo intentaba acceder al CD solo podía leerlo, no podía ejecutar programas "remotamente", o copiarme archivos del CD, cuando lo podía hacer con el HD sin ningún problema, tiempo después por suerte me di cuenta que el problema estaba en el nombre con el que yo compartía el CD, le cambie el nombre y funcionaba perfectamente, de igual manera este problema puede pasar con directorios, si la computadora se llama pepe y existe un directorio pepe e intentas acceder a él puedes tener problemas. Entre los trucos que te puedo decir de red con WIN-95 es: .- Si no vas a utilizar TCP/IP en la red, utiliza solo NETBEUI y déjalo como protocolo predeterminado, te va a dar mas velocidad. Si la computadora tiene módem, y esta en red puedes dejar TCP/IP solo en el acceso telefónico a redes (quita el de la tarjeta de red), te va a dar mas velocidad.

2.3.- BUSCAR UN PC EN LA RED

Si el usuario trabaja en una red y desea averiguar la direccion IP de otro ordenador de la misma red ejecute internet explorer y en address :

scriba // [y el host del ordenador]

propio win95 presenta una aplicación que nos muestra esta información, así como la máscara,...

Inicio->Ejecutar-> WINIPCFG

12.4.- BUSCAR UN PC EN LA RED (2).

Otra manera con Win95 de saber los IPs de otras maquinas y que no requiera de Internet Explorer es ir al DOS y alli hacer un PING a la computadora deseada. Ej.

```
c:\ping server1
```

```
ó
```

```
c:\ping administracion
```

y la maquina que te devuelva el ping sera su IP. Es un poco lenta la respuesta pero sirve perfectamente.

Y para los que les guste un poco UNIX existe un comando llamado "nslookup" que si le das el IP te devuelve el dominio y si le das el dominio te devuelve el IP. Existen varias aplicaciones graficas que hacen esto para Win95

12.5.- CREAR DISCO DE INICIO INSTALACIÓN CLIENTES MS CON PROTOCOLO NETBEUI

Como crear con un solo disco y que este sea de arranque, un cliente de redes Microsoft que estén configuradas con el protocolo NETBEUI, o también para copiar todos los archivos a un directorio del HD

Es de mucha utilidad, ya que podremos acceder a recursos compartidos de ordenadores WFW 311, W95, NT (aun no he probado con OS/2, ni LINUX corriendo con el SAMBA). Por ejemplo cuando queremos instalar el W95 en ordenador que no tiene CD-ROM, podemos acceder a otro que lo tenga. O también queremos acceder a un ordenador para ejecutar un determinado programa, o copiarnos algo, o imprimir en la impresora del otro ordenador, etc.

Esto siempre y cuando no tengamos instalado el wfw311 o el w95, ya que si los tuviéramos utilizaríamos el comando NET.

Los comandos de utilización de la red, son los utilizados por el cliente de dichos entornos para el S.O. MS-DOS. Este es el NET. Para saber mas sobre el solo es necesario poner:

```
NET /?
```

12.6.- CONECTAR 2 PC CON CABLE UTP O TP SIN CONCENTRADOR(HUB).

Como sabemos las conexiones deben ser normalizadas usándose generalmente la 568A, es decir en el conector RJ45 de 8hilos conectamos

PIN CABLE

- 1 BLANCO/NARANJA
- 2 NARANJA
- 3 BLANCO/VERDE
- 4 AZUL
- 5 BLANCO/AZUL
- 6 VERDE
- 7 BLANCO/MARRON
- 8 MARRON

para conectar dos PC con un cable sin hub debemos armar un conector normalizado en un extremo y en el otro armarlo de la siguiente manera:

PIN CABLE

- 1 BLANCO/VERDE *
- 2 VERDE *
- 3 BLANCO/NARANJA *
- 4 AZUL
- 5 BLANCO/AZUL
- 6 NARANJA *
- 7 BLANCO/MARRON
- 8 MARRON

Con placas Ethernet 10baseT de 10mbps obtenemos esta velocidad y si tenemos 100BaseT, la performance es incomparable, ahora resta esperar la llegada de GigaEthernet, promesa realizada por 3Com para fines de este semestre...

P.D.: Los materiales utilizados son AMP (conectores y cables) pero lo importante es respetar el orden de las conexiones mas allá de los códigos de color, el resto es solo configurar la red con protocolo NetBEUI o IPX/SPX (o por que no TCP/IP????), es a gusto (como la sal y los condimentos...) y por supuesto compartir los recursos en una u otra PC... (o ambas...)

Espero sea también útil a todos los lectores que tengan inquietud de conectar sus maquinas y/o transferir archivos de una a otra sin mayores costos. En realidad les mando el armado de un cable para puerto paralelo con dos conectores DB25 macho para poder utilizar la herramienta que viene en Windows'95, se encuentra en la carpeta accesorios y se llama conexión directa por cable.

En cuanto al armado de cables aquí va el detalle. Primero necesitas dos conectores DB25 normalizados (es decir standard) machos, y no mas de cinco metros de cable multipar para datos con no menos de once hilos (debes tener cuidado en este punto, ya que tienes que utilizar cables y no alambre por lo que te aconsejo "sacrificar" un cable de impresora del tipo centronics) y el armado del mismo quedaría mas o menos así:

Conector 1 Conector 2

pin 2	<----->	pin 15
pin 3	<----->	pin 13
pin 4	<----->	pin 12
pin 5	<----->	pin 10
pin 6	<----->	pin 11
pin 15	<----->	pin 2
pin 13	<----->	pin 3
pin 12	<----->	pin 4
pin 10	<----->	pin 5
pin 11	<----->	pin 6
pin 25	<----->	pin 25 (Tierra-Tierra)

12.7.- CONECTAR UN PC MSDOS CON UNO WINDOWS95/98.

Ante todo necesitamos los discos del Cliente para redes Microsoft. Para ello es necesario disponer de un Windows NT Server, ya que con este sistema podemos crear clientes de diversos sistemas operativos, entre el que se encuentra el DOS de Microsoft. Una vez tenemos los dos discos de cliente Microsoft (v 3.0 o superiores) que hemos creado con Windows NT Server, podemos pasar a la instalación del cliente en el ordenador con MS-DOS.

Introducimos el primer disco y hacemos "instalar", durante la instalación se nos pedirán los drivers de la tarjeta de red, los protocolos que queremos usar y la definición del grupo de trabajo y estación.

Recordatorio :

Nombre de usuario : Nombre que identifica dentro de un grupo de trabajo un usuario.

Nombre de computadora : Nombre que identifica nuestra máquina dentro de un grupo de trabajo.

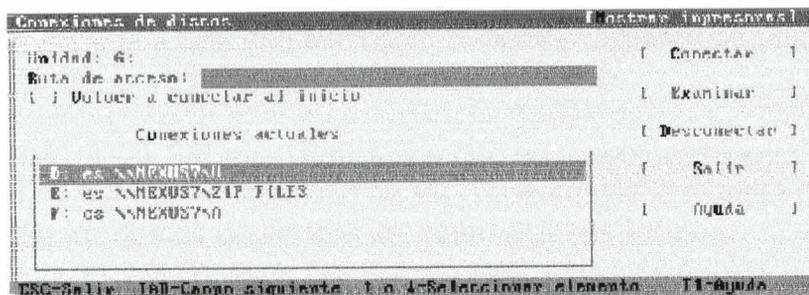
Nombre del grupo de trabajo : Es el nombre del conjunto de ordenadores al que pertenecemos.

Nombre de dominio : Identifica el dominio de Microsoft Windows NT o Lan Manager en el cual deseamos iniciar una sesión.

Una vez finalizado el proceso se reinicializará la máquina y nos pedirá que le entremos tanto el nombre de usuario como la contraseña (este último podemos dejarlo en blanco, és más, lo aconsejamos).

Ahora viene la parte interesante. Con los comandos net podemos conectarnos a un servidor, ¿cómo?.

Tan fácil como escribir el comando net, en la línea de comandos del DOS. En él aparecerá una pantalla similar a la siguiente:



Si conocemos la ruta de acceso podemos escribirla directamente, sino escogemos examinar, y nos aparecerá en la ventana superior el equipo servidor y en la inferior los directorios compartidos.

A simple vista podemos ver que si deseamos tener una conexión fija activaremos " Volver a conectar al inicio", de otra forma perderemos la unidad remota cuando apaguemos el equipo.

Algunos comandos de interés son :

net use : Nos da información del estado de la unidad, nombre local y nombre remoto.

net config : Visualiza nombre del PC, nombre de usuario, directorio raíz y grupo de trabajo.

```
C:\NET>net use

Estado          Nombre local      Nombre remoto
-----
Desconectado    D:                \\NEXUS7\H
Desconectado    E:                \\NEXUS7\ZIP FILES
Cancelado       F:                \\NEXUS7\A
El comando se completó con éxito.

C:\NET>net config
Computadora          \\SITE\SA
Nombre de usuario    SITE\SA

Versión del software 3.11
Versión del redirec... 2.51
Directorio raíz      C:\NET

Grupo de trabajo     ZAGADKA
El comando se completó con éxito.

C:\NET>
```

12.8.- CONECTAR VARIOS PC A UNA RED

Para conectarse a una Red Microsoft, debemos disponer de una tarjeta Ethernet compatible NE2000. Si ya la tenemos podemos empezar.

En Panel de Control --> Sistema verificamos que no tengamos ningún conflicto con la tarjeta de Red. Si hubiese un conflicto de IRQ buscaremos la manera de solucionarlo, combinando con los demás periféricos las interrupciones libres.

El siguiente paso, es ir a Panel de Control --> Red, hacemos doble Click.

Empezamos a agregar los componentes necesarios.

Agregamos cliente

Escogemos Microsoft -- > Cliente para Redes Microsoft.

Protocolo. Microsoft -----> Protocolo IPX/SPX por si tenemos intención de jugar al Quake o a otro juego que permita multijugador.

Protocolo. Microsoft -----> Protocolo TCP/IP por si queremos montarnos nuestra propia Intranet.

Opcionalmente -----> Protocolo NETBeui. Sirve para mensajería.

Finalmente. En servicios podemos escoger, compartir archivos e impresoras.

Durante la instalación se nos pide que debemos proporcionar un nombre al equipo con el que nos conectaremos y un nombre del grupo de trabajo.

Para esto, podemos dar a nuestra máquina cualquier nombre(Ojo con los caracteres raros ! !), y para el grupo de trabajo, el que este activo en la Red o proporcionaremos el que nosotros queramos crear.

Conectar varias impresoras NetPort o JectDirect

Tarjeta adaptadora que sirve para conectar una o hasta tres impresoras en la red consiguiendo que la impresora sea un host más de la red.

Por un lado tienen conectores a red (normalmente RJ-45) y por el otro salidas de impresión (normalmente paralelo aunque también las hay serie o ambas a la vez). Las de HP se llaman JetDirect y las de Intel NetPort.

La ventaja de estas impresoras se encuentra en la velocidad, ya que las redes de área local son mucho más rápidas que los puertos de comunicación o impresión de los ordenadores. Pueden usar diferentes protocolos (IPX, TCP/IP, DLC....) y pueden ser externas o internas (a la impresora). La mayoría tienen 3 leds, **Conectado, Actividad** de la red y **Fallo**.

Llevar consigo un software de configuración (en HP es llamado JetAdmin y para Intel NetPort) que se instala en cualquier estación y permite que pueda identificar las impresoras y capturarlas para su posterior uso como si de un puerto local del ordenador se tratase.

Inicialmente, si pretendemos usar TCP, deberemos de asignarle una IP a través del software de configuración en los 5 minutos (aproximadamente) de encender el JetDirect, de no ser así, se auto configura y normalmente toma el valor 192.0.0.192.

Para configurar el puerto de impresión en red, debemos de conocer la dirección MAC o dirección hardware o dirección física de la tarjeta (12 cifras hexadecimales). Las de HP empiezan por 080009xxxxxx donde los 6 primeros números los escogen las compañías. Actualmente HP ha adquirido otro nuevo rango de estas direcciones dado que ya había agotado las que con el anterior número podía tener en el mercado. Este número se halla bien en la documentación de la placa de impresión de red, bien en la misma placa o haciendo un autotest, esto es hacer que el JetDirect envíe una página con su propia configuración a la impresora que a él este conectada pulsando el botón que para ello lleva incorporado.

Para que nos hagamos una idea del coste de estos aparatos junto a sus respectivos programas de configuración, damos un par de precios referentes a HP, que son algo mas caros que los de Intel.

12.10.- IDENTIFICAR UN USUARIO DE UNA MAQUINA.

Si deseas identificar una maquina (nombre del usuario que esta ocupando una maquina determinada) por medio de un IP. esta es la forma:

En prompt de MS-DOS escribes lo siguiente: nbtstat_-A_y el IP.

12.11.- SINCRONIZAR LOS RELOJES DE LOS PC DE UNA RED.

Sirve tanto para Windows 95, 98 y NT

Desde el Menú Inicio, Ejecutar, y teclear el siguiente mandato:

```
net time \\computadora /set /yes
```

donde "computadora" es el nombre del sistema u ordenador con el que se desea sincronizar el reloj del nuestro.

Tan solo hay que ejecutarlo y nuestro reloj interno marcará exactamente la misma hora que la del otro.

Si se necesita hacerlo a menudo, no hay mas que abrir el bloq de notas y escribir la línea de comando anterior y salvar el archivo con extensión BAT. Se puede hacer un acceso directo en el escritorio y ejecutarlo desde alli cuando se quiera.

Si se desea sincronizar automáticamente su reloj cada vez que se ponga en marcha Windows, deberá crearse un acceso directo con este mandato y situarlo en la carpeta Inicio, dentro del Menú Inicio.

En WinNT, tiene la pega de que hay que estar como usuario Administrador para que nos deje modificar la hora del reloj, lo cual es un engorro si los otros puestos de la red trabajan a nivel de usuario. Desconozco si existen otros perfiles dentro de NT que permitan modificar la hora sin necesariamente ser Administrador.

Existe una forma de que una estación NT pueda modificar (y con ello sincronizar) la hora, a pesar de no ser administrador.

Si el administrador "LOCAL" nos modifica el "plan de derechos de usuarios" de "administrador de usuarios" en "herramientas administrativas"

Añadiendo al derecho de cambiar la hora del sistema, agregamos el perfil del usuario "todos" o el que convenga.

Ojo el administrador tiene que entrar en la estación como administrador local.

12.12.- ENVIAR MENSAJES ENTRE TERMINALES DE UNA RED.

Si se trabaja en una red en Windows 95 es muy fácil enviar mensajes entre una y otra terminal, solo busca una aplicación llamada Winpopup dentro de C:\WINDOWS\WINPOPUP.EXE y úsala es muy fácil e intuitiva.

12.13.- JUGAR EN RED SIN ENTRAR EN WINDOWS 95-98.

Para jugar en red no es necesario entrar dentro del modo gráfico de W95, sino que, teniendo ya instalada, configurada y comprobada la red, y utilizando el truco anterior, o la opción "Sólo símbolo de sistema" en el menú de inicio (que aparece pulsando F8 al iniciar el sistema), podemos cargar el IPX e incluso acceder a las unidades del otro ordenador. Para más información consultar el archivo C:\WINDOWS\NET.MSG

- La instrucción para cargar los protocolos y poder jugar en red con el protocolo IPX es NET START NWLINK, la cual se puede poner en el AUTOEXEC.BAT, precedida del comando LH.
- Para poder usar las unidades del otro ordenador (especialmente útil con el CD-ROM), crear un RED.BAT que esté dentro de uno de los directorios del PATH (creo que es necesario que el otro ordenador esté ejecutando W95).
- Primera instrucción: NET LOGON /Y
- Segunda instrucción: NET USE (X:) \\(YY)\(ZZZ). Donde: (X:) es la primera letra de unidad libre dentro del sistema. (YY) es el nombre en la red del otro equipo. (ZZZ) es el nombre del recurso compartido.
- (la instrucción anterior se repetirá tantas veces como unidades existentes a las que queramos acceder)

Estos trucos han sido probados con las versiones 950, 950a y 950b de W95 y la versión de actualización de W98; es posible que no todas las tarjetas de red permitan el segundo truco, pero por intentarlo no se pierde nada.

Ejemplo de RED.BAT

@ECHO OFF

NET START (sólo si no se ejecutó anteriormente el comando NET START NWLINK)

NET LOGON /Y

NET USE G: ||AZKON_1|C-MAESTRO

NET USE H: ||AZKON_1|D-MAESTRO

NET USE I: ||AZKON_1|CD-ROM

12.14.-ACELERAR CONEXIONES A RED.

Mezcla de win95 y win98

Aunque parezca lógico, no lo es. Si quieres ahorrar problemas de comunicación en una red con servidores de win95 y win98, NO utilices Netbeui. Por algún motivo, la filosofía de trabajo de win98 es distinta, sobretodo si trabajas con aplicaciones que mantengan ficheros abiertos, ya que win98 cierra la conexión con netbeui (también con ipx). Utilizad únicamente tcp/ip.

La red va muy lenta y se pierden las conexiones con RJ45 y con coaxial funciona bien.(Novell, Nt, Win, etc). Repasa la configuración de las tarjetas de red (en el disco de todas las tarjetas hay un setup) y aseguraros de DESACTIVAR la opción de FULLDUPLEX (a menos que tengáis un hub que lo soporte que son la minoría).

Mezcla de NT's y Win9x's

En propiedades de la red, en compartir recursos, deja solamente UNA máquina (normalmente el NT central o primero en encenderse) con la opción de examinador principal de dominio como activado o auto. En las otras máquinas la opción debería estar como desactivado. Se ahorran bastantes desconexiones de unidades solicitadas por las terminales sin que el servidor se entere.

Para acelerar conexiones y búsquedas usando IPX (Win9x, Nt's, Novell, etc)

Acostumbrados en las propiedades del protocolo IPX en la pestaña de avanzado, usar únicamente un solo tipo de trama (802.2 o 802.3) para evitar que en cada broadcast que se mande, se tenga que mandar con todos y cada una de las tramas. Es divertidísimo ver como al ponerlas en marcha todas de golpe, tienes 3 pc's usando una trama, 2 mas otra, etc, en cambio forzando una trama disminuyes el tráfico de paquetes por el cableado aumentando la eficacia y velocidad.

Optimización de protocolos. (Win9x, Nt's, Novell, etc)

Igual que el punto anterior, si se comunican con un protocolo, ¿Para que quieres usar dos?. Elimina todos los protocolos innecesarios. Si tienes tcp/ip, netbeui y ipx, dejando solo tcp/ip tienes que la información que circula por el cableado es un tercio. Imagínate que cada vez que buscas un PC, la información se manda en cada uno de los protocolos por separado (la máquina que buscamos no sabemos en que va a contestar), aparte de que todos los equipos tendrán que leer esos paquetes para saber si son para ellos o no.

Un recordatorio: Las velocidades del cableado, NO son lentas. Es lenta la información que hacemos circular por ella.

Evita el instalar programas compartidos con grandes ejecutables. Si montáis el word en red, cada vez que se pone en marcha circulan por el cableado varios megas de datos que nos podríamos ahorrar.

Un último consejo para los servidores NT: Si queréis que funcione bien, solo tienes que hacer 2 cosas: poner el doble de la ram que teníais prevista (de 128 hacia arriba) y NO usar el central como puesto de trabajo (bastante tiene haciendo de servidor).

Espero que estos pequeños trucos sean de ayuda a mas de uno.

Piensa que las redes pueden tener 3 opciones: baratas, rápidas y fiables pero solo puedes usar 2 a la vez.

- Una red barata y rápida no es fiable.
- Una red barata y fiable no es rápida.
- Una red rápida y fiable no es barata.

12.15.- ADMINISTRAR UN PC WIN95 DESDE OTRO TERMINAL SIN TENER EL PC COMPARTIDO (SHARED).

Como Administra una PC en una Red Windows 95 desde otra Terminal, sin necesidad de tener la PC Compartida (Shared).

Puedes acceder todos los recursos de una PC desde otra sin tener que compartir el o los discos, ni las impresoras. Para hacer esto entras a Control Panel, escoges la opción Passwords y te mueves a la tableta que dice Remote Administración, luego marcas donde dice Enable Remote Administración y asignas el password para Administrador que tendra esta PC (esto se lo haces a todas las PC's de tu area de trabajo y desde la tuya puedes corregir errores, compartir/descompartir discos, printers e incluso hacer correcciones de disco (Scandisk) y chequear si tiene virus.

Después de asignar el pase y desde tu estación entras a Network Neighborhood, seleccionas la PC que deseas administrar, le das click con el botón derecho y escoges propiedades, luego cambias a la Tableta Tools y escoges el Botón Adminístrate, luego te pedirá el password para Remote Administración (aquí pones el pass de Administrador que pusiste por Control Panel/Passwords/Remote Administración), marcas la casilla que dice Save This Password in your Password List, y listo, tienes acceso a todos los recursos de esa PC.

Esto particularmente lo hago porque soy el soporte técnico de mi Departamento, y así me evito estar parado a las demás estaciones cuando les surge algún inconveniente. Esto solo aplica a estaciones que ejecuten Windows 95 o Windows 98, no se puede para Windows 3.11 for Workgroups ni para Windows NT Workstation.

12.16.- DIFERENCIA ENTRE PROTOCOLO NETBEUI Y TCP/IP.

Solo quería aclarar cual es la diferencia entre el protocolo NETBEUI y el TCP/IP en una red. La diferencia esta en que el protocolo NETBEUI cuando hace un envío de paquetes lo que hace es enviarlo para una maquina en especial, pero no sabe en que lugar se encuentra, de esta forma, el paquete empieza a dar toda la vuelta por todas las maquinas, y si por esas casualidades (que son bastantes) la maquina destino esta ocupada haciendo otra tarea, entonces el paquete sigue dando vueltas y ocupando ancho de linea hasta que la maquina se libere y lo tome. En cambio el TCP/IP lo que hace al mandar el paquete para la maquina xxx.xxx.xxx.xxx, y solo hace un camino, sin que el paquete quede circulando por la red varias veces. Esta diferencia en la lentitud de la red, solo se nota si hay muchas maquinas conectadas, si uno esta usando 4 o 5 maquinas no notaria la diferencia.

12.17.- UTILIZAR LAS MISMAS BASES DE MENSAJES OUTLOOK EXPRESS EN TODOS LOS PC.

¿ Como utilizar las mismas bases de mensajes de Microsoft Outlook Express en todos los ordenadores conectados a una red local ?

Supongamos que hay varios ordenadores conectados a una red, todos con acceso a Internet, pero queremos que la base de mensajes sea la misma en todos los ordenadores. (Bandejas de Entrada, Salida, Elementos Enviados...etc.....)

Hay que acceder al registro del sistema, donde Outlook guarda la ruta completa de la ubicación de la base de mensajes, en cada ordenador al que queremos que se muestre la misma base de mensajes que en el servidor.

Puede hacerse de esta forma

- 1- Ir a Inicio y Ejecutar
- 2- Escribir regedit.exe y pulsar Aceptar para acceder al Registro del Sistema
- 3- Abrir esta clave: HKEY_CURRENT_USER\Software\Microsoft\Outlook Express
- 4- El Valor Store Root nos muestra la ubicacion de la base de mensajes, por ejemplo:
C:\WINDOWS\Application Data\Microsoft\Outlook Express
Aquí solo sería necesario cambiarlo por la ubicacion de la base de mensajes de la unidad que actua como servidor de red, por ejemplo:
F:\WINDOWS\Application Data\Microsoft\Outlook Express

12.18.- ENVIAR Y RECIBIR MENSAJES CON TODOS LOS PC DE LA RED CON SAMBAR.

Les envié una forma que descubrí para poder enviar y recibir mails desde las demás PC's.

editar el archivo config.ini que se encuentra en c:\sambar41\config en las sección [server] reemplazar:

Act As SMTP Proxy = false

Act As POP3 Proxy = false

por:

Act As SMTP Proxy = true

Act As POP3 Proxy = true

y mas abajo donde dice:

SMTP Server = smtp.ix.netcom.com

POP3 Server = smtp.ix.netcom.com

deberan reemplazarlo por:

SMTP Server = smtp.xx.com

POP3 Server = pop.xx.com

donde xx son las direcciones de los servidores que Uds. poseen

Ej.

SMTP Server = smtp.ethek.com

POP3 Server = pop.ethek.com

luego cuando configuran la cuenta en el outlook express u otro soft de correo desde los puestos remotos deberá colocar todos los datos que correspondan realmente salvo las direcciones de los servidores entrante y saliente

En ambos casos deberán colocar la dirección IP que le dieron a la PC que ejecuta el sambar server (siguiendo el ej de la pagina de trucos:10.10.10.10)
Aun no pude descubrir como hacerlos en el caso de tener distintos servidores SMTP Y POP
(por ej una cuenta común y otra del tipo mypad.com) , pero es cuestión de seguir adelante.

12.18.- HACERSE UN TERMINADOR IMPROVISADO.

Cuando urge un terminador y no se dispone de uno solo hay que poner en su lugar una resistencia de 50 oms 1/2w.

12.19.- CONCLUSIONES.

Los trucos aquí indicados no son mas que secretos o experiencias personales que ha surgido de la necesidad de los clientes y usuarios de red, asi mismo no quiere decir que son todos los existentes pero si son de lo mas practicos es recomendable que todo usuario de red vaya haciendo su pequeño manual propio de redes para asi tener a la mano la informacion cuando le sea requerida, asi como tambien anotar en dicho manual las experiencias y situaciones dificiles encontradas a lo largo de intalacion, supervision, configuracion y administracion de redes locales.

Estoy conciente de que existe mucho mas trucos de lo aquí mencionados pero seria tema de trabajo de investigacion bastante redundante ya que asi como existe tipos de microprocesadores existen sistemas operativos, los cuales tienen sus trucos, recomendaciones y algo mas.

CAPITULO 13

RECOMENDACIONES.

Las recomendaciones para tener una red optima bajo algún sistema operativo Microsoft, es la elección de los equipos adecuados, con la versión del sistema operativo ideal para ese sistema, así como las configuraciones necesarias y completas en los equipos de la red local.

El requerimiento mínimo de sistema de computo en una red local Microsoft es el requerimiento mínimo de Windows 95, que es una computadora 486, 8 mb. Pero se recomienda 16 mb como mínimo, 60 mb en disco duro, recomendado 200 mb. Ranuras de expansión ISA para T. red 10 Mbps y PCI para T. red de 100 Mbps, es en lo respecta a lo de sistema informático.

Para una red local es muy importante la red eléctrica ya que sin esta no es posible, además debe ser con la capacidad necesaria, esto es usar lo cables con el calibre adecuado para el numero de componentes instalados así como la pastilla de protección debe ser de los amperes necesarios, para evitar con la inestabilidad de la corriente eléctrica que se active la protección de la pastilla.

Para la instalación en un local nuevo debe tener en cuenta el numero de computadoras y componentes que se van a instalar, cuando esta ya existe y se va ampliar se debe conocer a fondo las especificaciones técnicas instalación existente, y no olvidar lo importante que es la tierra física así como la instalación de reguladores con pila para conservar como mínimo 10 minutos la energía para así lograr cerrar y guardar los programas o sistemas. Siempre documentando un manual para estos casos en cada uno de los equipos de la red ya que puede estar compartiendo algún recurso en la red.

Además del cableado eléctrico, es el cableado de red es muy importante ya que este debe ser lo mas extendido posible, y el cable debe ser blindado, ya que muchas vez desconocemos que tanta interferencia existe en el lugar donde esta situado nuestra red, así como la instalación de canaletas haciendo lo mas discreta nuestra instalación y el trayecto del cable, para así evitar maltrato o por que no hasta el rompimiento del cable.

Recuerde el principio de que las redes pueden tener 3 opciones: baratas, rápidas y fiables pero solo puedes usar 2 a la vez.

- Una red barata y rápida no es fiable.
- Una red barata y fiable no es rápida.
- Una red rápida y fiable no es barata.

Se deben hacer respaldo de la información importante, para así mismo evitar la pérdida o el borrado accidental de las principales y más importante Programas así como actualizaciones bajadas de Internet, para así en un caso de restauración del sistema, sea mejor y mas rápido, ya que una terminal fuera de la red es pérdida de tiempo y dinero y lo menos que se tarde la restauración es menos la pérdida.

Por ultimo la documentación de tu red es como la radiografía para el doctor solo así se puede resolver con el mínimo de trabajo y tiempo algún problema y situación dentro de la red, así como una bitácora de situaciones presentadas con la administración y configuración de la red local, por que es posible que se pueda volver a presentar el hecho nuevamente.

14. - CONCLUSIONES.

Con la instalación de una red local, conseguimos reducir los costos de grandes equipos de hardware (impresoras láser, sistemas de backup grandes, etc.) y otros equipo que al necesitar solo uno de ellos para la red en la cual puede haber desde 2 hasta miles de terminales conectados usando esos equipos de hardware de modo común, nos ha permitido el no tener que comprar un equipo de hardware para cada ordenador que tengamos, reduciendo así increíblemente los costos.

Al estar la información en continuo movimiento y uso permitimos una constante actualización de datos en tiempo real, evitando así el continuo uso de disquetes para poner en cada ordenador lo que ha codificado uno de ellos en un programa concreto, siendo la actualización de ficheros rápida y más eficaz.

El único inconveniente que puede presentarse al necesitar montar una red es posiblemente el desembolso inicial al realizar dicha instalación de equipo pero ganando en productividad y fiabilidad de los datos que en la red estemos utilizando.

Hoy en día la euforia de Internet, la creación de espacios para los usos de redes locales conectadas a Internet, se ha hecho algo de todos los días, pasar por cualquier calle o poblado cercano y ver un letrero con grandes y remarcadas letras: **INTERNET**. Que no es otra cosa la interconexión de grandes redes locales.

La era de las redes existe, mas adelante vendrá la era de los beneficios de la conjugación de los medios, como: e-commerce, accesos móviles inalámbricos, etc.

Con la culminación este proyecto logro el que muchas personas como yo que tienen el particular interés y curiosidad por las redes, encuentren una referencia sólida en este trabajo como un principio de su red,

Cabe señalar que los conocimientos vaciados aquí son la captación de experiencia y conocimientos la mayoría de ellos probados, con casos prácticos.

Por ultimo en la actualidad los avances de la tecnología son demasiados cortos, uno nunca acaba de tener lo ultimo, cuando ya existe algo mas nuevo y de mejores características, así mismo es el desarrollo de software para redes(NOS), uno no acaba de explotar todas las características del software, cuando ya tenemos la nueva versión, en una red tal vez no se ocupe de lo ultimo hay que explotar lo existente, y partir con lo que se cuenta, ya que como objetivo principal de una red es reducir costos.

ACRONIMOS GENERALES.

A	
AAS	American Astronomical Society
ABI	Application Binary Interface
ANSI	American National Standards Institute
API	Application Program Interface
APPC	Advanced Peer to Peer Communications
APPN	Advanced Peer-to-Peer Network
ARCNet	Attached Resource Computer Network
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ASCII	American Standard Code for Information Interchange
ASICs	Application-Specific Integrated Circuits
AT	Advanced Technology
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
B	
BBN	Bolt, Beranek and Newman
BCP	Binary Compatibility Package
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BIOS	Basic Input/Output System
C	
CCITT	Consultive Committee on International Telephone and Telegraph
CDE	Common Desktop Environment
CD-ROM	Compac Disc-Read Only Memory
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTAN	Comprehensive TeX Archive Network
CTL	Complex Text Layout
COPS	Computer Oracle and Password System
CRC	Cyclical Redundancy Check
CTIO	Cerro Tololo Image Observatory
D	
DARPA	Defense Advanced Research Projects Agency
DDI/DKI	Device Driver Interface/Device kernel Interface
DDN	Defense Data Network
DDP	Datasys dedicated Port
DDX	Device-Dependent X
DGA	Direct Graphics Access
DHTML	Dynamic Hypertext Markup Language
DIG	Domain Information Groper
DIP switch	Dual-In Package switch
DLC	Data Link Control
DLSw	Data Link Switching

DMA	Direct Memory Access
DNS	Domain Name System
DoD	Department of Defense
DOS	Disk Operating Systems
DPP	Distributed Packet Processing
DPS	Display PostScript System
DR	Dynamic Reconfiguration
DS1	Digital System 1
DS3	Digital System 3
DS4	Digital System 4
DTE	Data Terminal Equipment
E	
ECC	Error Correction Code
ECF	European Coordination Facility
ECMA	European Computer Manufacturers Association
EPROM	Erasable Programable Read Only Memory
EEPROM	Electrically Erasable, Programable Read Only Memory
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
EIS	Executive Information System
EISA	Extended Industry Standard Architecture
ELF	Executable and Linking Format
EOF	End Of File
EOT	End Of Transmission
F	
FAT	File Allocation Table
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FITS	Flexible Image Transport System
FOIRL	Fiber Optic Inter Repeater Link
FTP	File Transfer Protocol
G	
GAN	Global Area Network
GBICs	Gigabit Interface Converters
GNN	Global Network Navigator
GUI	Graphical User Interface
H	
HDLC	High Data Level Control
I	
IAB	Internet Activities Board
IAU	International Astronomical Union
ICCCM	Inter Communication Conventions Manual
ICMP	Internet Control Message Protocol
IDE	Integrated Device Electronics
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFM	Intelligent Flow Management

IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IIIMP	Internet Intranet Input Method Protocol
IIS	International Imaging System
IKI	Image Kernel Interface
IOS	Internetworking Operating System
IP	Internet Protocol
IPAC	Infrared Processing and Analysis Center
IPC	InterProcess Communication
IPSec	Internet Protocol Security
IPX	Internet Packet eXchange
IRAF	Image Reduction and Analysis Facility
IRAS	Infrared Astronomy Satellite
IRC	Internet Relay Chat
IRTF	Internet Research Task Force
ISA	Industrial Standard Application
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU	International Telecommunication Union
L	
LAN	Local Area Network
LASER	Light Amplification by Stimulated Emission
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emission Diode
LLC	Logical Link Control
LU	Logical Unit
M	
MAC	Medium Access Control
MAU	Multi Access Unit
MCA	MicroChannel Adapter
MHC	Multiple Hardware Color maps
MIDAS	Munich Image Data Analysis System
MII	Media Independent Interface
MIME	Multipurpose Internet Mail Extension
MIT	Unshielded Twisted Pair
MOSPF	Multicast Open Shortest Path First
MPG	Multiple Plane Groups
MTU	Maximum Transmission Unit
N	
NDIS	Network Driver Interface Specification
NFS	Network File System
NFSNET	National Science Foundation Network
NIC	Network Information Center
NIS	Network Information Services
NLM	Netware Loadable Module
NLSP	NetWare Link Services Protocol

NNI	Network to Network Interface
NNTP	Network News Transport Protocol
NOAO	National Optical Astronomy Observatories
NOS	Network Operating System
O	
OCR	Optical Character Recognition
ODI	Open Data-link Interface
OEM	Original Equipment Manufacturers
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P	
PACE	Priority Access Control Enable
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PDF	Portable Document Format
PDN	Public Data Network
PIC	Position-Independent Code
PING	Packet Internet Groper
POSIX	Portable Operating System Interface for Computer Environments
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PROM	Programable Read Only Memory
R	
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RAP	Roving Analysis Port
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RDI	Integrated Services Digital Network
RFC	Request for Comments (Read for Confuse)
RIP	Routing Information Protocol
ROM	Read Only Memory
RPC	Remote Procedure Call
RTFM	Read The Fine Manual
S	
SAA	System Application Architecture
SAC	Single Attachment Concentrator
SAP	Service Advertisement Protocol
SCA	Single Connector Attachment
SCO	Santa Cruz Operation
SCSI	Small Computer System Interface
SDAS	Science Data Analysis System
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SLIP	Serial Line Internet Protocol
SMCC	Sun Microsystems Computer Company
SMDS	Switched Multimegabit Data Service

SMS	Storage Management Services
SMTTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SPOOL	Simultaneous Peripheral Operations On Line
SPX	Secuencial Packet Exchange
SQL	Structure Query Language
SSP	System Service Processor
STA	Spanning Tree Algorithm
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
STScI	Space Telescope Science Institute
T	
TCP	Transmission Control Protocol
TELNET	Virtual Terminal
TP	Twisted Pair
TPI/DLPI	Transport Provider Interface/Data Link Provider Interface
U	
UDP	User Datagram Protocol
UNI	User Network Interface
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus
USL	Unix System Laboratories
UUCP	Unix to Unix Copy Protocol
V	
VAR	Value Added Resealler
VERONICA	Very Easy Rodent Oriented Netwide Index to Computerized Archives
VESA	Video Electronics Standard Arquitecture
VINES	Virtual Networking System
VLAN	Virtual LAN
VMS	Virtual Memory System
W	
WAIS	Wide Area Information Server
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WWW	World Wide Web
WYSIWYG	What You See Is What You Get
Y	
YP	Yellow Page.

1

10-100

(O *10+100*) Hace referencia a un dispositivo que tiene ambas conexiones, 10Mbps Ethernet y 100Mbps Fast Ethernet, en puertos separados. Contrasta con 10/100, que tiene las conexiones en el *mismo* puerto.

Consultar también 10/100, autonegociación, Ethernet, Fast Ethernet, Mbps, puerto.

10/100

Hace referencia a un dispositivo que tiene ambas conexiones, 10Mbps Ethernet y 100Mbps Fast Ethernet, en el mismo puerto. Contrasta con 10-100, que tiene las conexiones en puertos *diferentes*.

Consultar también 10-100, autonegociación, Ethernet, Fast Ethernet, Mbps, puerto.

10 BASE-T

Esta es una especificación técnica que se utiliza en redes Ethernet. 10 BASE-T forma parte de la especificación del organismo de estándares IEEE para Ethernet (10Mbps) sobre las Categorías 3, 4 o 5 de cable de par trenzado (dos pares de cables - un par para transmitir datos y el segundo para recibirlos). 10 BASE-T tiene un límite de distancia por segmento de 100m (328 pies) aproximadamente.

Ver también: cables de la categoría 3, cables de la categoría 5, Ethernet, IEEE, Mbps, par trenzado, red, segmento, STP, UTP.

10 BASE2

10 BASE 2 forma parte de la especificación del organismo de estándares IEEE para Ethernet 10Mbps, y es un cable coaxial delgado, también conocido como *thinnet* o *cheapernet*. 10 BASE 2 tiene un límite de distancia por segmento de 185m aproximadamente (607 pies).

Ver también: cable coaxial, Ethernet, IEEE, Mbps, red, segmento.

10 BASE5

Esta es una especificación técnica utilizada en las redes Ethernet. 10 BASE 5 forma parte de la especificación del conjunto de estándares IEEE para Ethernet 10Mbps, y es un cable coaxial grueso. 10 BASE 5 tiene una distancia límite por segmento de 500m (1640 pies) aproximadamente.

Ver también: cable coaxial, Ethernet, IEEE, Mbps, red, segmento. Esta es una especificación técnica utilizada en las redes Ethernet.

10 BASE-FL

forma parte de la especificación del conjunto de estándares IEEE para utilizar cable de fibra óptica de 10Mbps (Ethernet). Los segmentos de una red que utilizan cables de 10 BASE-FL pueden ser de hasta 2km (1.24 millas) de longitud.

Ver también: cable de fibra óptica, IEEE, Mbps, red, segmento.

100 BASE-FX

Esta es una especificación técnica utilizada en las redes Fast Ethernet. 100 BASE-FX forma parte de la especificación del conjunto de estándares IEEE para utilizar cable de fibra óptica de 100Mbps (Fast Ethernet).

Ver también: cable de fibra óptica, Ethernet, Fast Ethernet, IEEE, Mbps, red.

100 BASE-TX

Esta es una especificación técnica utilizada en las redes Fast Ethernet. 100 BASE-TX forma parte de la especificación del conjunto de estándares IEEE para cable (2 pares de cables - un par para transmitir datos y el segundo para recibirlos) de la Categoría 5 UTP (par trenzado no blindado) o STP (par trenzado blindado) de 100Mbps (Fast Ethernet).

Ver también: cables de Categoría 5, Ethernet, Fast Ethernet, IEEE, Mbps, red, STP, UTP.

56K

Designación utilizada para describir un dispositivo compatible con el estándar V.90 ITU para ejecutar descargas de 56 Kbps.

Ver también: Kbps, ITU.

A

ADAPTADOR DE CORRIENTE

Un adaptador de corriente es un transformador que convierte la corriente alterna (CA) de un enchufe de pared, en corriente continua (CC), como requieren los dispositivos electrónicos.

ADAPTADOR DE TERMINAL

Dispositivo utilizado en una red RDSI para conectar a un solo usuario al exterior.

Ver también: RDSI.

ADSL

Línea **S**ubscriptora **D**igital **A**simétrica. Línea de teléfono que transfiere datos a alta velocidad. La parte "asimétrica" quiere decir velocidades diferentes de transmisión, desde el cliente a la compañía telefónica, de hasta 640 Kbps, y desde la compañía telefónica al cliente de 1.544 a 6.1 Mbps.

Consultar también [DSL](#), [Kbps](#), [Mbps](#), [xDSL](#).

ANCHO DE BANDA

El ancho de banda es una medición de la capacidad de información de un enlace de comunicación. Ethernet, por ejemplo, tiene un ancho de banda de 10Mbps.

Decimos de aquellos usuarios de estaciones de trabajo o de redes, que utilizan la red de un modo intenso, que utilizan un *ancho de banda alto* - estos usuarios realizan habitualmente muchos trabajos con gráficos o de multimedia a través de la red.

El ancho de banda es la diferencia entre la frecuencia más alta y la frecuencia más baja de un enlace de comunicación, y se mide en Hertz (Hz).

Ver también: [Ethernet](#), [Mbps](#), [red](#).

ATM

Ver [Modo de Transferencia Asíncrono](#).

AUI

Interfaz de **U**nidad **C**onectada. Esta es una interfaz IEEE 802.3 (Ethernet) estándar que le permite conectarse a un PC, o conectar un dispositivo Ethernet a una red Ethernet. Es posible que su PC tenga una NIC (tarjeta de interfaz de red) con un zócalo AUI de 15 pines.

Ver también: [Ethernet](#), [IEEE](#), [NIC](#), [PC](#), [red](#), [transceptor](#).

AUTODETECCIÓN

Algunos dispositivos de la gama soportan la auto-sensing. En este caso es cuando un puerto que puede operar a velocidades diferentes (por ejemplo, 10Mbps y 100Mbps), tiene la capacidad de detectar la velocidad de otro puerto al cual está conectado; ambos puertos se configurarán automáticamente para utilizar la mejor velocidad común. Este término y *autonegociación* se usan indistintamente, ya que ambos son similares.

Ver también: [autonegociación](#), [Mbps](#), [puerto](#).

AUTONEGOCIACIÓN

Algunos dispositivos soportan la negociación automática o autonegociación.

La negociación automática se da cuando dos dispositivos que comparten el mismo enlace, se configuran automáticamente para utilizar la velocidad más adecuada para ambos. El orden de preferencia (el mejor es el primero) es: 100 BASE-TX full dúplex, 100 BASE-TX semidúplex, 10 BASE-T full dúplex, y 10 BASE-T semidúplex. La negociación automática se define en el estándar IEEE 802.3 para Ethernet, y es una operación que se desarrolla en unos pocos milisegundos.

Ver también: [100BASE-TX](#), [10BASE-T](#), [dúplex](#), [full dúplex](#), [IEEE](#), [red](#), [semidúplex](#).

B

BAUDIO

Es la velocidad *indicadora* de una línea; en otras palabras, la velocidad a la que los datos viajan a través de una línea. Baudio es el número de transiciones (cambios de voltaje o de frecuencia) hechas por segundo.

Ver también: [bps](#).

bit

Dígito binario. Es el elemento más pequeño de información del ordenador. Un bit es un único dígito en un número binario (0 o 1). Los grupos de bits forman unidades más grandes de datos en los sistemas de ordenador - siendo el byte (ocho bits) el más conocido de éstos.

Ver también: [bps](#), [byte](#).

BNC

Conector **N**aval **B**ritánico. Los conectores BNC se utilizan para conectar, extender o terminar redes de cables coaxiales, como es Ethernet. Algunos concentradores tienen un puerto BNC.

Hay varios conectores, como son el conector BNC T, el conector BNC cilíndrico y el terminador BNC.

Ver también: [10 BASE 2](#), [cable coaxial](#), [puerto](#), [transceptor](#).

BPS

bits por segundo. bps se utiliza como medición de transmisión de datos en un sistema de comunicaciones.

Ver también: [bit](#), [Kbps](#), [Mbps](#).

BRIDGE

Los bridges ofrecen un modo de juntar dos o más redes para formar una red lógica única, y son similares a los conmutadores. Las redes que se juntan son conocidas en la red resultante como *segmentos de red*. Los bridges pueden conectar LANs (Redes de área local) de un tipo de red diferente, como por ejemplo, Ethernet a Fast Ethernet, o Ethernet a Token Ring.

Los bridges se pueden instalar en redes por las siguientes razones:

Para aumentar el tamaño o el número de nodos de la red entera.

Para reducir embotellamientos de tráfico causados por un número excesivo de nodos.

Para enlazar tipos diferentes de redes, tales como Ethernet y Token Ring, y enviar paquetes entre ellas.

Ver también: [conmutador](#), [Ethernet](#), [Fast Ethernet](#), [LAN](#), [nodo](#), [paquete](#), [red](#), [segmento](#), [Token Ring](#), [tráfico](#).

BUCLE DE RED

El bucle de red ocurre cuando dos componentes de un equipo de una red están conectados por más de una ruta, por lo que los paquetes circulan alrededor de la red constantemente sin llegar a su destino. Un concentrador repetidor detecta los bucles de red y automáticamente divide uno de sus puertos para abrir el bucle.

Ver también: [concentrador](#), [división](#), [paquete](#), [red](#).

BYTE

Es una unidad de datos equivalente a ocho dígitos binarios (bits). Un byte contiene el equivalente a un carácter único, como puede ser una letra del alfabeto (*a*) o un signo de y (&). Las medidas de los dispositivos de almacenamiento, tales como discos y bases de datos, se dan en bytes.

Ver también: [bit](#).

C

CABLE COAXIAL

Es un cable de red de alta capacidad. El cable coaxial (o *coaxial*) consiste en una funda hueca blindada con cobre trenzado o metal, rodeando un único conductor de cobre interno con aislamiento plástico entre las dos capas conductoras. El cable coaxial se utiliza en redes de comunicación de banda ancha (como es, por ejemplo, el cable de televisión) y cables de banda base (como es, por ejemplo, Ethernet). El cable coaxial no se ve habitualmente afectado por interferencias externas, y es capaz de lograr altas velocidades de transmisión en largas distancias.

Ver también: [red](#), [STP](#), [UTP](#).

CABLE CON EMPALME

Este tipo de cable tiene sus cables conectados a las mismas pines en ambos extremos (los cables de emisión y de recepción incluidos). Para que funcione una conexión entre dos dispositivos, el receptor de uno de ellos debe de estar conectado al emisor del otro dispositivo. Por lo tanto, al conectar un puerto Normal (MDI-X) a un puerto Enlace ascendente (MDI), se debe utilizar un cable con empalme. Este tipo de cable es el más común de los cables fabricados disponibles para networking.

Ver también: [MDI/MDI-X](#), [Enlace ascendente/Normal](#), [puerto](#),

CABLE CRUZADO

Un cable cruzado tiene cruzados sus cables de recibir y de emitir. Para que funcione una conexión entre dos dispositivos, el receptor de uno de ellos debe de estar conectado al emisor del otro dispositivo.

Por lo tanto, hay que utilizar un cable cruzado al conectar dos puertos MDI o dos puertos MDI-X.

Ver también: [EIA/TIA-232](#), [MDI](#), [PC](#), [puerto](#).

CABLE DE CAT3

Ver [cables de la categoría 3](#).

CABLE DE CAT5

Ver [cables de la categoría 5](#).

CABLE DE FIBRA ÓPTICA

Cable que contiene una, o más de una, fibra óptica y que se utiliza para transmitir datos en forma de luz. El cable de fibra óptica es más caro que el cobre, pero no es susceptible a interferencias electromagnéticas, y es capaz de velocidades de transferencia de datos más altas en distancias mayores.

CABLE DÚPLEX

Cable que contiene un canal de emisión (Tx) y un canal de recepción (Rx).

Ver también: [full dúplex](#), [semidúplex](#).

CABLE MODEM

Módem utilizado para conectar un ordenador a un sistema de TV por cable que ofrezca servicios en línea.

Ver también [módem](#).

CABLES DE LA CATEGORÍA 3

Es uno de los cinco grados de cables de par trenzado (TP) definidos por el estándar EIA/TIA-586. El cable de la Categoría 3 es un cable de calidad telefónica que se utiliza en las redes 10 BASE-T (Ethernet) para transmitir datos a velocidades de hasta 10Mbps.

Ver también: 10 BASE-T, cables de la categoría 5, EIA, Ethernet, Fast Ethernet, Mbps, par trenzado, red, TIA.

CABLES DE LA CATEGORÍA 5

Es uno de los cinco grados de cables de par trenzado (TP) definidos por el estándar EIA/TIA-586. El cable de la Categoría 5 se utiliza en las redes 100 BASE-T (Fast Ethernet) y puede transmitir datos a velocidades de hasta 100Mbps. El uso de los cables de la categoría 5 es más indicado para las redes que los de la Categoría 3, porque soportan ambas velocidades, la de Ethernet (10Mbps) y la de Fast Ethernet (100Mbps).

Ver también: 100 BASE-T, cables de la categoría 3, EIA, Ethernet, Fast Ethernet, Mbps, par trenzado, red, TIA.

CANAL B

Canal portador En comunicaciones RDSI, un canal B transmite comunicaciones a 64 Kbps.

Ver también: canal D, Kbps, RDSI.

CANAL D

Canal de señalización en una línea RDSI, utilizado para transportar mensajes entre un módem RDSI y el conmutador público. Transmite a 16 o 64 Kbps.

Ver también: canal B, RDSI, Kbps.

CAPA 1

En las comunicaciones RDSI, esta es la 'capa' física de comunicación entre el equipo de comunicaciones, según el modelo de referencia OSI. Si la capa 1 no está activa, no se podrá establecer la conexión RDSI entre los dispositivos.

Ver también: RDSI, modelo de referencia OSI.

CERTIFICACIÓN DE CLASE A/B

Esta es la certificación FCC (Comisión Federal de Comunicaciones) de límites de radiación aplicados a los dispositivos digitales. Clase A es para el uso en el sector de negocios. Clase B es para el uso residencial, y es más rigurosa con el fin de evitar interferencias con televisores y otros aparatos receptores.

Ver también: FCC

CHAP

Protocolo de autenticación de desafío. Protocolo utilizado para verificar un nombre de usuario y una contraseña durante las conexiones PPP.

Ver también: PAP, PPP.

Clase I/II

Según las normas que definen las redes de Fast Ethernet (IEEE 802.3u), los dispositivos de redes están clasificados. Esto quiere decir que dos concentradores de la Clase II se pueden conectar entre sí directamente, mientras que los concentradores de la Clase I no pueden.

Ver también: Ethernet, Fast Ethernet, concentrador, IEEE

CLIENTE

Es un sistema de ordenador o de estación de trabajo que solicita un servicio o los contenidos de un fichero desde un servidor de ficheros.

Ver también: cliente/servidor, red cliente/servidor, servidor.

CLIENTE/SERVIDOR

Es una arquitectura de red por la que se divide un sistema en dos partes: el cliente (terminal frontal) es un ordenador solicitante (normalmente un PC), y el servidor (terminal final), es un ordenador suministrador. Ambos términos se pueden aplicar a los dispositivos de hardware o a los programas de software.

Ver también: cliente, red, red cliente/servidor, servidor

COAXIAL DELGADO

Ver también: 10 BASE 2.

COAXIAL GRUESO

Ver también: 10 BASE 5.

CODIFICACIÓN

Es el proceso de codificar datos durante su transmisión para impedir que sean accedidos por un usuario no autorizado.

COLISIÓN

Término utilizado para describir dos paquetes que colisionan en una red Ethernet o Fast Ethernet. Las colisiones son parte de una operación normal de Ethernet o de Fast Ethernet, pero un repentino incremento prolongado en el número de colisiones puede indicar un problema con un dispositivo, particularmente si no vienen acompañadas por un aumento general en tráfico. En los segmentos coaxiales, un incremento en las colisiones puede indicar cables defectuosos.

Ver también: cable coaxial, Ethernet, Fast Ethernet, paquete, tráfico.

CONCENTRADOR

Un concentrador (hub) sirve como una ubicación central para conectar ordenadores y otros dispositivos (como impresoras) entre sí. Un concentrador es llamado a veces "repetidor multipuerto", porque pasa, o repite, todos los paquetes que recibe a todos sus puertos.

Ver también: conmutador, paquete, repetidor.

CONGESTIÓN

Tráfico de red excesivo.

Ver también: red, tráfico.

CONMUTADOR

Un conmutador (switch) solamente envía información cuando es necesario (a diferencia del concentrador, que envía información a todos sus puertos). Una vez que aprende qué dispositivos pueden alcanzarse a través de cada puerto, el conmutador solamente pasará paquetes a los puertos adecuados. De este modo, un conmutador puede reducir la cantidad de tráfico en gran medida, y mejorar el rendimiento de la red.

Ver también: concentrador.

CONTROLADOR DE RED

Es software que controla un puerto, como es por ejemplo una tarjeta de interfaz de red (NIC), un teclado, una impresora o un monitor. El equipo de red (como por ejemplo los concentradores) conectado a los PCs, necesita controladores que el PC utiliza para comunicar con ellos.

Ver también: NIC, PC, puerto.

CORREO ELECTRÓNICO

Correo electrónico. Es la transmisión de mensajes a individuos o grupos a través de una red. Los mensajes por correo electrónico pueden contener mensajes de texto, tablas, gráficos, imágenes, y también ficheros vinculados. El uso del correo electrónico en un entorno de oficina puede reducir el uso del papel, ya que los memos y la comunicación interna se envía a través de la red, por lo que se ahorra tiempo y caros materiales de oficina.

Ver también: red.

CSMA/CD

Acceso Múltiple del Sentido de Portadora con Detección de Colisión. Este es el protocolo definido en las normas de Ethernet y Fast Ethernet (IEEE 802.3), en el que los dispositivos emiten solamente tras encontrar un canal de datos vacío durante un período de tiempo. Una colisión ocurre cuando los dos dispositivos transmiten simultáneamente, y los dos dispositivos involucrados en la colisión retrasan la emisión durante un período aleatorio de tiempo.

Ver también: colisión, Ethernet, Fast Ethernet, IEEE, protocolo

D

DATAGRAMA

Es un mensaje TCP/IP o IPX que contiene direcciones fuente y de destino de Internet y datos que se utilizan para encaminar un paquete a través de una red. Datagramas son las unidades de información primaria que se utilizan en Internet

Ver también: Internet, TCP/IP.

DBA

Asignación dinámica de ancho de banda. DBA es un método de reasignar ancho de banda (como un canal B automáticamente). DBA le permite hacer o recibir llamadas de voz mientras hay una llamada Multilink PPP en activo.

Ver también: ancho de banda, canal B, Multilink PPP.

DHCP

Protocolo de control dinámico de host. Windows 95, 98 y NT contienen software que asigna direcciones IP a estaciones de trabajo en una red. Estas asignaciones se hacen a través del software del servidor DHCP que se ejecuta en el servidor Windows NT Server; Windows 95 y 98 llamarán al servidor para obtener la dirección. Windows 98 se asignará una dirección a sí mismo, si el sistema no puede encontrar un servidor DHCP.

Ver también: dirección IP, servidor.

DIAFONÍA

Es la interferencia en un cable o en una pieza componente de un equipo, creada por una señal en un cable o en una pieza componente de un equipo adyacente. La diafonía puede afectar a la calidad de transmisión de datos.

DIFUSIÓN

Un paquete de datos enviado por un dispositivo a todos los nodos en una red, o *dominio de difusión*.

Ver también: [difusión](#), [multicast](#), [paquete](#), [red](#), [unicast](#).

DIFUSIÓN TORMENTA

Son las difusiones simultáneas múltiples, que típicamente absorben ancho de banda de red disponible, y pueden provocar que se enlentezca una red o que no se pueda utilizar. Un broadcast puede ocurrir, por ejemplo, porque el equipo de red está defectuoso.

Ver también: [ancho de banda](#), [difusión](#), [red](#).

DIRECCIÓN DE SUBRED

Extensión del esquema de obtención de direcciones IP, por medio del cual un sitio puede utilizar una dirección de red IP sencilla para múltiples redes físicas.

Ver también: [IP](#), [red](#).

DIRECCIÓN IP

La dirección de Protocolo de internet es la dirección de la capa de la red de un dispositivo asignado por el usuario o administrador de red de una red IP. Una dirección IP consiste en 32 bits divididos en dos o tres campos: un número de red y un número de host, o un número de red, un número de subred y un número de host.

Ver también: [bit](#), [IP](#), [red](#).

DIRECCIÓN MAC

Dirección de control de acceso medio; también se conoce por dirección de hardware o dirección física. Es una dirección asociada con un dispositivo de red en particular. Los NICs y dispositivos gestionados que se conectan a una LAN tienen una dirección MAC asignada a los mismos, ya que las direcciones MAC se utilizan para identificar dispositivos en una red. Las direcciones MAC tienen 6 bytes de longitud, están especificadas por el IEEE y vienen preasignadas a su equipo de red.

Ver también: [byte](#), [dispositivo gestionado](#), [IEEE](#), [LAN](#), [NIC](#), [MAC](#), [red](#).

DISPOSITIVO GESTIONADO

Los dispositivos gestionados son aquellos que soportan la gestión de redes.

Ver también: [gestión de redes](#)

DISPOSITIVO NO GESTIONADO

Son aquellos que no soportan gestión de red.

Ver también: [gestión de redes](#)

DNS

Sistema de Denominación de Dominio. DNS traduce un nombre alfabético común en su dirección IP numérica. Un servidor DNS permite a los usuarios localizar ordenadores en Internet, manteniendo una base de datos de nombres de host y direcciones IP.

Ver también: [dirección IP](#), [Internet](#), [nombre de dominio](#).

DSL

Línea Subscriptora Digital. Tecnología para facilitar información de ancho de banda alta a usuarios residenciales y pequeños negocios, a través de líneas telefónicas normales de cobre.

Ver también: [ancho de banda](#).

DUAL SPEED HUB

El Dual Speed Hub 8 y el Dual Speed Hub 16 son concentradores fáciles de utilizar con 8 o 16 puertos del tipo 10/100 BASE-TX. Cada puerto se puede conectar a un dispositivo Ethernet o Fast Ethernet. Cada puerto detecta automáticamente la velocidad del dispositivo conectado y opera a la mayor velocidad posible.

Ver también: [10/100](#), [Ethernet](#), [Fast Ethernet](#)

DÚPLEX

Es una transmisión que permite establecer una comunicación en dos sentidos. Dúplex es sinónimo de full dúplex.

Ver también: [full dúplex](#), [semidúplex](#).

E

EIA

Asociación de **Industrias Electrónicas**. Es una organización de comercio industrial que, junto con TIA (Asociación de la Industria de la Telecomunicación), define las normas de los productos eléctricos. EIA y TIA especifican las normas de transmisión de datos tales como EIA/TIA-232.

Ver también: [EIA/TIA-232](#), [TIA](#).

EIA/TIA-232

es una norma para una interfaz en serie de 25 pines, que se puede utilizar para conectar ordenadores a componentes que forman parte de una red. (EIA/TIA-232 se denominaba anteriormente RS-232.)

Ver también: [EIA](#), [red](#), [TIA](#).

EMC

Compatibilidad electromagnética. Es la capacidad de un dispositivo para operar efectivamente en el entorno para el que estaba destinado, sin recibir interferencias electromagnéticas (EMI) provenientes de otros dispositivos o equipos, o generarlas.

ENCAMINADOR

Los encaminadores facilitan un enlace entre redes separadas geográficamente. Una interconexión de redes basada en encaminamientos consiste en muchas subredes lógicas diferentes. Los bridges y conmutadores conectan estas subredes, y su función es mejorar el rendimiento de la red manteniendo el tráfico dentro de los segmentos. Los repetidores y concentradores enlazan segmentos entre sí, y las estaciones de trabajo en los segmentos.

Ver también: [bridge](#), [concentrador](#), [conmutador](#), [red](#), [segmento](#), [tráfico](#).

ENLACE

Conexión física entre dos nodos en una red.

Ver también: [nodo](#), [red](#).

ENLACE ASCENDENTE/NORMAL

Es el interruptor situado en la parte trasera de un conmutador o concentrador que se utiliza para alterar la operación de un puerto específico. Un puerto Enlace ascendente (sin cruzar) se conecta al puerto Normal (cruzado) de otro concentrador.

A continuación, podrá ver un ejemplo de la utilización del interruptor Enlace ascendente/Normal.

- Empezando desde abajo, conecte el puerto con la numeración más alta del concentrador más bajo de la pila a cualquier puerto del concentrador inmediatamente superior. Repita este paso por cada concentrador.
- Disponga todos los interruptores Enlace ascendente/Normal en Enlace ascendente (dentro), exceptuando el concentrador más alto (aquél que tenga el puerto con la numeración más alta sin conectar a otro concentrador). Este puerto no utilizado podrá conectarse a un PC siempre que el interruptor Enlace ascendente/Normal esté dispuesto en Normal (fuera).

Ver también: [cable con empalme](#), [concentrador](#), [conmutador](#), [MDI](#), [MDI/MDIX](#), [puerto](#).

ESPECIFICACIÓN DE INTERFAZ DE CONTROLADOR DE RED (NDIS)

Especificación de software utilizada en algunos sistemas operativos de red (como pueden ser LAN Manager y Windows NT), para crear controladores para adaptadores de red. Los controladores NDIS soportan protocolos y adaptadores múltiples.

Ver también: [controlador](#), [NOS](#), [protocolo](#).

ETHERNET

Xerox Corporation inventó Ethernet, y lo desarrolló conjuntamente con Intel, y Digital Equipment Corporation (DEC), y es una tecnología utilizada extensamente en las LANs.

Las redes de Ethernet utilizan el protocolo CSMA/CD y funcionan en varios cables a una velocidad de 10Mbps; son utilizadas, por ejemplo, por protocolos TCP/IP y XNS. Ethernet es similar a una serie de normas producidas por IEEE, conocidas como IEEE 802.3.

Ver también: [CSMA/CD](#), [Fast Ethernet](#), [IEEE](#), [LAN](#), [Mbps](#), [protocolo](#), [TCP/IP](#), [XNS](#).

F

FAST ETHERNET

opera a una velocidad de 100Mbps y por lo tanto tiene un ancho de banda 10 veces mayor que Ethernet, lo cual le permite hacer frente a mayores cantidades de tráfico; como resultado de esta mayor velocidad, la operación se realiza 10 veces más rápidamente que en Ethernet. Fast Ethernet funciona a través de los diferentes (cables) 100 BASE: por ejemplo, 100 BASE-FX y 100 BASE-TX.

Las redes de Fast Ethernet operan a una velocidad de 100Mbps, y se basan en el método de acceso a red 10 BASE-T Ethernet CSMA/CD, extensión de la norma IEEE 802.3.

Ver también: [10 BASE-T](#), [100 BASE-TX](#), [100 BASE-FX](#), [ancho de banda](#), [CSMA/CD](#), [Ethernet](#), [IEEE](#), [Mbps](#), [red](#), [tráfico](#)

FCC

Comisión Federal de Comunicaciones. Es el organismo regulador de las telecomunicaciones de los EE.UU., que licencia y controla las normas de transmisiones electrónicas y electromagnéticas. FCC especifica gamas de anchos de banda para canales de comunicación diferentes.

FDDI

Interfaz de fibra de datos distribuidos. Es una norma de red para las transmisiones a través de cable de fibra óptica de alta velocidad. FDDI utiliza dos anillos de cables de fibra óptica (que ofrecen mayor resistencia) y transmite en distancias entre nodos de hasta 2km (1.24 millas) a una velocidad de 100Mbps. FDDI se utiliza generalmente a modo de *tecnología principal*, por medio de la cual se puede efectuar una conexión entre redes Ethernet y Token Ring. Se utiliza en aplicaciones críticas como, por ejemplo, en un aeropuerto.

Ver también: cable de fibra óptica, Ethernet, LAN, Mbps, nodo, paquete, principal, protocolo, servidor, Token Ring.

FILTRADO

Es un proceso en el que se filtra el tráfico de red en busca de ciertas características, tales como la dirección de destino (dirección del dispositivo al que está destinado el paquete) o protocolo. De este proceso se determina si el tráfico se emite basado en los criterios establecidos. De esta manera se permite cruzar el bridge al tráfico de interconexión de redes esencial solamente, por lo que de este modo se reduce el tráfico de interconexión de redes. El filtrado en los encaminadores puede evitar un acceso no autorizado a una red o a un sistema principal en una red; esta barrera es generalmente conocida como *muro corta fuego*. Los bridges, conmutadores, y los encaminadores ejecutan el filtrado.

Ver también: bridge, conmutador, encaminador, interconexión de redes, paquete, protocolo, red, tráfico.

FIREWALL

Un firewall en una red es un nodo configurado como una barrera para impedir que el tráfico cruce de un segmento a otro. Los firewalls se utilizan para mejorar el tráfico, y a modo de medidas de seguridad, y pueden hacer las veces de una barrera entre redes públicas y redes privadas conectadas. Se puede implementar un firewall en un encaminador o puede ser un dispositivo de red especial para este propósito.

Ver también: encaminador, nodo, red, segmento, tráfico.

FRAME RELAY

Frame relay es un protocolo de conmutación de paquetes de alta velocidad utilizado en redes WAN. Es popular en las conexiones LAN to LAN a lo largo de distancias remotas, y está indicado para transferir datos e imágenes. Debido a su arquitectura de paquete de longitud variable, no es la tecnología más eficiente para transmitir voz y vídeo. Frame Relay es más popular en los EE.UU. que en Europa.

Ver también: LAN, Modo de Transferencia Asíncrono, paquete, red, WAN.

FUERZA DE TRABAJO DE INGENIERÍA DE INTERNET (IETF)

Comité que revisa y respalda propuestas de protocolos de Internet.

Ver también: protocolo.

FULL DÚPLEX

Es la capacidad de un dispositivo o de una línea de transmitir datos simultáneamente en ambas direcciones a través del mismo enlace de comunicaciones, con lo que potencialmente se duplica el rendimiento total del tráfico.

Ver también: ancho de banda, cable dúplex, semidúplex.

G

GATEWAY

Dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles. El Gateway ejecuta una conversión de protocolo para traducir un conjunto de protocolos en otro conjunto de protocolos (por ejemplo, de TCP/IP a IPX).

Ver también: IPX, modelo de referencia OSI, protocolo, red, TCP/IP.

GESTIÓN DE RED

A medida que su red crece, puede que sea necesario *gestionar* las comunicaciones de la misma. Esto se conoce como gestión de red. Monitorizar una red le permite diagnosticar problemas y recoger estadísticas referentes al comportamiento de la red, para administrarla mejor.

Ver también: concentrador, conmutador, dispositivo gestionado, red.

GIGABIT ETHERNET

Gigabit Ethernet es una extensión de los estándares IEEE 802.3 Ethernet de 10 Mbps (Ethernet) y 100 Mbps (Fast Ethernet). Gigabit Ethernet opera a una velocidad de 1000 Mbps y mantiene una compatibilidad absoluta con la base instalada de nodos Ethernet.

Ver también: Ethernet, Fast Ethernet, Mbps, nodo, red.

H

HTML

Ver también: Lenguaje Hypertext Markup.

HIPERTEXTO

Palabra o frase en un documento en línea que se vincula a otra sección del mismo documento, o a un documento diferente. Las palabras o frases en hipertexto se muestran generalmente en azul y subrayadas.

I

IEEE

Instituto de Ingenieros Electricistas y Electrónicos. Esta organización se fundó en 1963 y define las normas referentes a ordenadores y comunicaciones. El comité que definió las 802 normas para ejecutar operaciones en red, se fundó en 1980 con el fin de garantizar que los sistemas y dispositivos fabricados por diferentes proveedores pudieran comunicar con la menor complicación posible, permitiendo de esta manera una compatibilidad global a través de los diferentes productos.

IGMP

Ver también: Protocolo de Gestión de Grupo de Internet.

INTELIGENCIA DISTRIBUIDA

Función de networking, por medio de la cual la potencia de procesamiento se distribuye entre varios dispositivos conectados que funcionan independientemente, mientras que continúan siendo operativos como parte de un sistema más amplio.

Ver también: cliente/servidor.

INTERCONEXIÓN DE REDES

Es un conjunto de redes (que pueden ser de tipos diferentes) que están interconectadas por medio de encaminadores, gateways, u otros dispositivos, para que de este modo puedan funcionar como una sola gran red. A veces se denomina internet, que es *diferente* a Internet (*la* World Wide Web).

Ver también: Encaminador, Internet, red, WWW.

INTERFAZ GRÁFICA DE USUARIO (GUI)

Una interfaz visual de ordenador que representa comandos, archivos y otras acciones informáticas con iconos, símbolos y cuadros de diálogo. Una GUI podría ser un interfaz de web.

INTERFERENCIA

Reduce la sobrecarga de la red por medio de la reducción de tráfico en una red WAN (como son las señales que informan repetidamente que un dispositivo está activo). El encaminador o bridge pueden comunicar a un dispositivo remoto que un dispositivo LAN está todavía encendido, en lugar de que el dispositivo LAN informe al dispositivo remoto de que sigue encendido.

Ver también: bridge, encaminador, LAN, tráfico, WAN.

INTERNET

Internet es una red global compuesta por redes gubernamentales, académicas, comerciales, militares y corporativas que abarcan todo el mundo.

Internet fue desarrollada originalmente por el ejército norteamericano, y poco después se popularizó en la investigación académica y comercial. Los usuarios que tienen acceso a Internet pueden leer y descargar datos, virtualmente acerca de cualquier tema, desde casi cualquier parte del mundo.

Ver también: intranet, red, WWW.

INTRANET

Las Intranets son redes privadas internas, utilizadas por compañías e instituciones académicas alrededor del mundo. El público del exterior no puede acceder a estas Intranets, que sirven como bases de datos de información en el mismo formato que utiliza la World Wide Web.

Ver también: internet, red, World Wide Web.

IP

Protocolo de internet. IP es un protocolo de red de la capa 3 (del modelo de referencia OSI), que es el protocolo estándar para enviar una unidad de datos básica (un datagrama IP) a través de una interconexión de redes. IP es parte del conjunto de protocolos TCP/IP que describen los encaminamientos de paquetes a dispositivos con dirección.

Ver también: datagrama, Internet, interconexión de redes, modelo de referencia OSI, paquete, protocolo, TCP/IP.

IPX

Intercambio de Paquetes Internet. Es un protocolo de comunicaciones diseñado por Novell para Novell NetWare. Los paquetes IPX se pueden encaminar de una red a otra en las capas 3 y 4 del modelo de referencia OSI.

Ver también: Internet, modelo de referencia OSI, paquete, red.

ISA

Los zócalos ISA miden unos 14 cms de largo y son Arquitectura de normas industriales; han sido estándar desde el primer PC. Se utilizan todavía en los PC modernos debido a la gran gama de tarjetas de expansión diseñadas para este zócalo.

Ver también: Ethernet, NIC, PC.

ISP

Proveedor de Servicios Internet. Compañía que facilita el acceso a Internet a organizaciones o usuarios individuales.

Ver también: Internet.

ITU

Unión Internacional de Telecomunicaciones. La organización desde la que gobiernos y el sector privado coordinan redes de telecomunicaciones e interfaces globales.

K

Kbps

Kilobits por segundo. Es la medida de la velocidad de transferencia de datos en un sistema de comunicaciones. Un kilobit equivale a 1000 bits.

Ver también: bit, Mbps.

L

LAN

Red de área local. Es una red de dispositivos conectados (como son PCs, impresoras, servidores y concentradores) que cubren un área geográfica relativamente pequeña (generalmente no más grande que una planta o un edificio). Las LAN se caracterizan por transmisiones de alta velocidad en cortas distancias. Ethernet, FDDI y Token Ring son tecnologías ampliamente utilizadas en la configuración de LANs.

Ver también: Ethernet, Fast Ethernet, FDDI, concentrador, red, servidor, Token Ring.

LANTastic

Este es un sistema operativo de igual a igual, desarrollado por la compañía Artisoft para redes Ethernet y Token Ring.

Ver también: Ethernet, red, redes de igual a igual, Token Ring.

LED

(DEL) **Diodo emisor de luz.** Es una fuente de luz semiconductor que emite luz por medio de la conversión de energía eléctrica.

Ver también: red

LED alerta

En todos los concentradores, hay una serie de LEDs (diodos emisores de luz) que suministran información acerca del estado del dispositivo.

Ver también: concentrador, LED red.

Lenguaje HyperText Markup (HTML)

Lenguaje utilizado para crear páginas en la World Wide Web.

Ver también: WWW.

LÍNEAS DEDICADAS

Una red carente de conexión, en la que se cobra al usuario una tarifa plana en lugar de costes de conexión o por minuto, asociada típicamente con llamadas de larga distancia.

M

Mac

Es la abreviatura de los ordenadores Macintosh.

MAC

Media Access Control. Es un protocolo para determinar aquellos dispositivos que tienen acceso a una red en cualquier momento determinado, especificado por el IEEE. El protocolo MAC difiere según sea el método utilizado para conectar la red (por ejemplo, Token Ring o Ethernet).

Ver también: dirección MAC, IEEE, Ethernet, protocolo, red, Token Ring.

MÁSCARA DE SUBRED

Término utilizado para indicar qué cantidad de una dirección IP se utiliza para identificar la red. Una dirección IP tiene dos partes: la primera identifica la red y la segunda identifica el ordenador o PC en la red.

Ver también: dirección IP, red.

Mbps

Megabits por segundo (no confundir con megabytes por segundo - *Mbps*). Es la medida de la velocidad de transferencia de datos en un sistema de comunicaciones. Un megabit es un millón de bits. Diez megabits por segundo (10Mbps) equivale a 10 millones de impulsos transmitidos por segundo en un sistema de comunicaciones.

Ver también: bit, MBps.

MBps

MegaBytes por segundo (no confundir con megabits por segundo - *Mbps*). Es la medida de la velocidad de transferencia de datos en un sistema de comunicaciones. Un megabyte equivale a un millón de bytes aproximadamente. [1 MB = 1,048,576 bytes.]

Ver también: byte, Mbps.

MDI

Interfaz dependiente del medio. MDI se refiere a una conexión de puerto Ethernet. La norma de red IEEE 802.3 define MDI como la interfaz eléctrica y mecánica entre un componente de equipo y un medio de transmisión. En un puerto RJ45, existe un línea de emisión y una línea de recepción. Los puertos RJ45 pueden ser MDI (las líneas no están cruzadas) o MDI-X (las líneas están cruzadas). Para que funcione una conexión entre dos dispositivos, el receptor de uno de ellos tiene que estar conectado al emisor del otro, por lo tanto, el puerto MDI de un dispositivo debe de estar conectado a un puerto MDI-X de otro dispositivo utilizando un cable con empalme. MDI se conoce también como Enlace ascendente, y MDI-X se conoce como Normal.

Ver también cable con empalme, IEEE, Enlace ascendente/Normal, Ethernet, MDI/MDIX, puerto, red, RJ-45.

MDI/MDI-X

Interfaz dependiente del medio/Interfaz dependiente del medio con puente de cruce. El interruptor, también conocido como Enlace ascendente/Normal, está situado en la trasera de un conmutador o concentrador que se utiliza para alterar la operación de un puerto específico. La 'X' indica el cruce de las líneas de transmisión y recepción de un puerto. Un puerto MDI (Enlace ascendente, sin cruzar) se conecta al puerto MDI-X (Normal, cruzado) de otro concentrador.

Ver también: concentrador, conmutador, MDI, puerto.

MODELO DE REFERENCIA OSI

Modelo de referencia de Interconexión de modelos abiertos. El modelo de referencia OSI es un estándar global de la industria, utilizado en las operaciones red, con el fin de definir cómo se comunican los protocolos a través de una red. El modelo de referencia OSI se desarrolló para ayudar a los desarrolladores a crear aplicaciones que sean compatibles en productos de distintas marcas.

Aprender las capas y funciones de OSI ayuda a entender las redes de comunicaciones.

Resumidamente, cuando un dispositivo en una red quiere comunicarse con otro enviando un mensaje (por ejemplo, un correo electrónico), el mensaje pasa a través de las capas del modelo. Cada una de las siete capas vincula instrucciones al mensaje, hasta que el paquete entero adopta una forma que puede pasar a través de la red. El mensaje es descifrado por el modelo a medida que el mensaje avanza a través de las capas hasta llegar a su destino final.

Ver también: concentrador, conmutador, encaminador, Ethernet, Fast Ethernet, Internet, red.

MÓDEM

MÓdulo de DEModulación. Es un dispositivo que adapta la señal digital de un ordenador en frecuencias de sonido (análogas) para transmitir a través de una línea de teléfono, y las adapta de nuevo a digitales. Las velocidades de transmisión de los módems se sitúan generalmente entre los 2.400bps (2.4Kbps) a los 56.000bps (56Kbps).

Ver también: bps, Kbps.

MODO DE TRANSFERENCIA ASÍNCRONO (ATM)

Modo de transmisión en el que la información se organiza en celdas. Las celdas tienen 53 bytes de longitud y acceden a la red a través de conexiones virtuales. Una red ATM utiliza estas conexiones virtuales para repetir el tráfico, a través de conmutadores de alta velocidad, desde el equipo de envío local del cliente (CPE) hasta el equipo de recepción local del cliente.

Ver también byte, conmutador, tráfico.

Multicast

Es un mensaje que se envía simultáneamente a un grupo de nodos específicos en una red.

Ver también: difusión, nodo, red.

Multilink PPP

Protocolo Punto a Punto **Multilink PPP** es un protocolo que facilita un método para combinar múltiples conexiones PPP. **Multilink PPP** agrega los dos canales RDSI B de 56 Kbps o 64 Kbps, creando de este modo una sola conexión digital virtual de 112 Kbps o 128 Kbps.

Ver también: canal B, Kbps, PPP, protocolo, RDSI.

Multiplexor

Dispositivo utilizado en líneas de comunicación, que actúa como un embudo transmitiendo señales de datos separadas a través de un sólo canal simultáneamente.

N

NAT

Traducción de **Direcciones de Redes**. NAT hace referencia al proceso de conversión de las direcciones IP utilizadas en una red privada a direcciones IP de Internet.

Ver también: dirección IP, Internet, red.

NDIS

Ver también: Especificación de Interfaz de Controlador de Red.

NetBEUI

Interfaz extendida del usuario **NetBIOS**. Esta es una versión mejorada del protocolo NetBIOS utilizado por un sistema operativo de red (NOS), como es por ejemplo Windows NT de Microsoft. NetBEUI se pronuncia "netbuui".

Ver también: LAN, NetBIOS, NOS, protocolo, red, trama.

NetBIOS

Entrada **básica de red/Sistema de salida**. Es un protocolo común de red para redes de área local (LANs) que contienen PCs (ordenadores personales).

NetBIOS es una norma de red establecida que provee la interfaz entre un sistema operativo de un PC y su canal de entrada/salida. NetBIOS se formalizó después en NetBEUI.

Ver también: LAN, modelo de referencia OSI, NetBEUI, NOS, PC, protocolo, red, trama.

NetWare

Es un sistema operativo de red (NOS) desarrollado por Novell. NetWare soporta DOS, Mac y UNIX, además de varias tecnologías de red LAN, tales como Ethernet, y Token Ring. Consultar NOS para obtener una descripción más detallada de los sistemas operativos de red.

Ver también: Ethernet, LAN, Mac, NOS, red, Token Ring, UNIX.

Network Ready

Es un nombre de marca registrado ordenadores personales que se fabrican con controladores preinstalados y una tarjeta de interfaz de red (NIC). Cada PC que lleva el logo Network Ready, está garantizado como operativo, virtualmente en cada entorno de sistema operativo de red.

Ver también: controlador, NIC, NOS, PC, red.

Network Terminator (NT-1)

Un NT-1 es un dispositivo de red que termina la línea RDSI.

Ver también: RDSI.

NIC

Network Interface Card, o Tarjeta de interfaz de red (también conocida como *adaptadora* o *tarjeta adaptadora*). Es una placa de circuito instalada en un componente de equipo de informática, como un PC, por ejemplo, que le permite conectar su PC a una red.

Ver también: PC, red.

NODO

Es un dispositivo conectado a una red, como puede ser un ordenador o un servidor.

Ver también: red, servidor.

NOMBRE DE DOMINIO

Dirección de una conexión de red (por ejemplo, www.yahoo.com) que identifica al titular jerárquico de la dirección.

Ver también: DNS.

NOS

Sistema operativo de red. Un sistema operativo de red es software que permite a los usuarios compartir ficheros, impresoras, faxes, módems y acceder a un servidor.

Los sistemas operativos de red gestionan recursos de red que pueden estar completamente autocontenidos (tales como NetWare), o requieren un sistema operativo existente para poder funcionar (LAN Manager requiere OS/2, y LANtastic requiere DOS). Ejemplos de sistemas operativos de red son Windows NT, Windows for Workgroups, Windows 95, Windows 98 y LANtastic.

Ver también: DOS, LAN, LANtastic, módem, NetWare(r), red, servidor.

NT-1

Un NT-1 es un dispositivo de red que termina la línea RDSI .

Ver también: RDSI.

O

OSI

Interconexión de sistemas abiertos. Son estándares de redes de ordenador desarrollados por ISO y CCITT (Comité Consultivo Internacional Telegráfico y Telefónico), con el fin de crear estándares comunes de comunicación entre ordenadores fabricados por diferentes marcas.

Ver también: modelo de referencia OSI, red.

OSPF

Abrir la Ruta más Corta Primero. Protocolo de encaminamiento de red, utilizado en redes IP como Internet , que localiza la ruta más corta a cada nodo de la red.

Ver también: Internet, IP, red.

P

PAQUETE

Un paquete es una unidad de información que se envían entre sí las estaciones de trabajo y otro equipo a través de la red. Cuando se envía información desde un ordenador (como puede ser un fichero de texto), se transmite a través de la red como una serie de paquetes.

Un paquete consiste en un conjunto de bits que forman un solo bloque de datos, y que contiene una cabecera formado por información de control como es el emisor, el receptor, y datos de control de errores, además del mismo mensaje. Debido a que son unidades de datos de red similares, los términos *paquete* y *trama* se utilizan indistintamente.

Ver también: bit, concentrador, conmutador, encaminador, red, trama.

PAP

Protocolo de Autenticación de Contraseña PAP es el protocolo que verifica un nombre de usuario y una contraseña en las conexiones PPP. Se utiliza este protocolo si el más extensivo CHAP no está disponible.

Ver también: CHAP, PPP, protocolo.

PAR TRENZADO (TP)

Es un par de cables delgados que se utilizan generalmente en los teléfonos y en las redes de ordenadores. Los cables están trenzados uno alrededor del otro para minimizar las interferencias provenientes de otros cables.

Los dos tipos de cables de par trenzado más importantes son los pares trenzados blindados (STP) y los pares trenzados no blindados (UTP). UTP es popular porque es más delgado y no ocupa mucho espacio, pero STP ofrece más protección contra interferencias electromagnéticas.

Ver también: ancho de banda, cable coaxial, cable de fibra óptica, cables de la categoría 3, cables de la categoría 5, red, STP, UTP.

PCI

Los zócalos PCI (de **Interconexión de componente periférico**) se utilizan en todos los PCs Pentium de sobremesa. Los zócalos PCI ofrecen un rendimiento mucho más completo que los ISA; este rendimiento es esencial para aprovechar al máximo las tarjetas de expansión de alto rendimiento de hoy en día. Los zócalos PCI miden unos 9cm de longitud.

Ver también: Ethernet, Fast Ethernet, ISA, Mbps, NIC, PC.

PCMCIA

Asociación internacional de tarjetas de memoria para PC. Esta organización no comercial se fundó en 1989 para formalizar un método de conexión de equipo a ordenadores portátiles.

Ver también: tarjeta de PC.

PING

Packet INternet Groper. Comprobación de la ruta entre el dispositivo gestionado y otro dispositivo en una red IP que responde a paquetes IP (Protocolo de Internet). Durante una comprobación de ping, el dispositivo gestionado envía paquetes de petición de eco ICMP (Protocolo de Mensaje de Control de Internet) a otro nodo con la dirección IP especificada, y espera a que regresen los paquetes de respuesta de eco. El nodo debe de ser capaz de recibir y responder a paquetes ICMP.

Ver también: [IP](#), [paquete](#), [protocolo](#).

POP

Punto de Presencia. Punto en una red WAN que conecta llamadas de teléfono locales a la red.

Ver también: [WAN](#).

POTS

Línea de Servicio Telefónico Normal. POTS es la conexión de teléfono básica a una red conmutada.

PPP

Protocolo Punto a Punto. PPP facilita un método estándar de establecer una conexión de acceso telefónico a Internet . PPP se utiliza para la comunicación entre un PC y un ISP.

Ver también: [Internet](#), [ISP](#), [Multilink PPP](#).

PPTP

Protocolo de túnel punto a punto. Protocolo por medio del cual una estación de trabajo puede establecer una conexión segura de protocolo múltiple a una red privada remota, a través de una llamada a un ISP local.

Ver también: [ISP](#), [protocolo](#), [VPN](#).

PRI

Primary Rate Interface. Una línea PRI es uno de los dos métodos de acceso a RDSI; BRI es el otro método. En Norteamérica, PRI está formada por 23 canales B de 64 Kbps y un canal D de 64 Kbps (conocidos como 23B+D). La PRI europea está formada por 30 canales B de 64 Kbps y un canal D de 64 Kbps (conocidos como 30B+D).

Ver también: [BRI](#), [canal B](#), [canal D](#), [Kbps](#), [RDSI](#).

PRINCIPAL

Cable principal que conecta segmentos de la red. Este cable lleva información entre dispositivos relativamente remotos, como por ejemplo, entre dos concentradores en dos lados opuestos de un mismo edificio.

Ver también: [concentrador](#), [segmento](#).

PROTOCOLO

En una red, un protocolo es un conjunto formal de normas y convenciones desarrollado por organismos reguladores internacionales que deciden cómo intercambian datos los distintos aparatos de una red. Un protocolo define el formato, la sincronización, el control y la secuencia de datos en una red.

Ver también: [red](#).

PROTOCOLO DE GESTIÓN DE GRUPO DE INTERNET (IGMP)

Protocolo utilizado por hosts de Internet para informar de sus afiliaciones de grupos de destinatarios múltiples a cualquier encaminador de destinatario múltiple de las cercanías. Debe implementarse por todos aquellos hosts que esperen recibir IP de destinatario múltiple. Los mensajes IGMP se encapsulan en datagramas IP. Los protocolos de destinatario múltiple son importantes cuando el usuario intenta reducir o limitar tráfico broadcast en la red. Los protocolos multicast también se utilizan cuando un usuario intenta ejecutar enseñanza de vídeo de difusión, a través de la red, a estudiantes específicos distribuidos a través de una red multisegmentada. En lugar de que todos reciban una corriente de vídeo, ésta es solamente dirigida a PCs en particular.

Ver también: [datagrama](#), [difusión](#), [encaminador](#), [Internet](#), [IP](#), [multicast](#), [protocolo](#), [red](#), [segmento](#), [tráfico](#).

PROTOCOLO DE INFORMACIÓN DE ENCAMINAMIENTO (RIP)

Proceso de mover un paquete de un nodo a otro, por medio del envío del paquete al siguiente encaminador.

Ver también: [encaminador](#), [paquete](#).

PROTOCOLO DE INTERNET DE LÍNEA EN SERIE (SLIP)

SLIP es un estándar de facto, utilizado generalmente para conexiones en serie punto a punto que ejecutan TCP/IP.

Ver también: [PPP](#), [protocolo](#), [TCP/IP](#).

PUERTO

Es un zócalo desde el que los datos pueden entrar y salir de un ordenador, o de un dispositivo componente de una red. En un ordenador personal, los puertos de serie (consola) y paralelos sirven para conectar líneas de comunicación a aparatos tales como módems, encaminadores e impresoras.

Ver también: encaminador, interconexión de redes, módem.

PUERTO COM

Puerto de comunicaciones en serie de un PC compatible con Windows.

R

RAS

Servidor de Acceso Remoto. Dispositivo en una red, compuesto por un banco de módems, por medio del cual los usuarios pueden conectarse a la red a través de líneas de acceso telefónico.

Ver también: módem, servidor.

RDSI

Red digital de servicios integrados. Es una norma de telecomunicaciones internacional para transmitir voz, vídeo y datos a través de líneas digitales que funcionan a 64Kbps. Se utiliza RDSI para redes privadas o públicas de teléfono digital en las que datos binarios, tales como gráficos y voz digitalizada y transmisión de datos, pasan a través de la misma red digital por la que corren la mayoría de las transmisiones de teléfono de hoy en día.

Ver también: Kbps, red.

RED

Es un grupo de dispositivos, como por ejemplo los ordenadores, las impresoras, los concentradores, los conmutadores, y otros componentes de hardware, que están conectados entre sí y pueden comunicar entre sí. Las redes varían en tamaño: Unas pueden abarcar una sola oficina, y otras abarcar todo el mundo.

Ver también: concentrador, conmutador, interconexión de redes, red.

RED CLIENTE/SERVIDOR

Es una estructura de red de área local (LAN), en la que los recursos de red están centralizados y controlados desde uno o más servidores. Las estaciones de trabajo individuales o *clientes* (como son los PCs) deben solicitar los servicios a través del/los servidor/es.

Ver también: cliente, cliente/servidor, LAN, PC, red, red de igual a igual, servidor, tráfico.

RED DE IGUAL A IGUAL

Una red de igual a igual es aquella en la que las estaciones de trabajo (como los PCs) pueden compartir información y los recursos de todos ellos, sin tener que depender de un servidor central. Por ejemplo, en una red de cuatro PCs y un concentrador, es posible permitir el acceso a los ficheros de los cuatro PCs desde cualquier otro PC.

Ver también: concentrador, PC, red, red cliente/servidor, servidor.

RED DE TELEFÓNICA CONMUTADA (RTC)

La red telefónica que se encuentra en todas partes del mundo. Está formada por teléfonos, cables RJ-11 de par trenzado, y la oficina central. La RTC también se conoce como POTS (servicio telefónico de línea normal). La razón principal por la que RTC no ha sido sustituida por una nueva tecnología, como es RDSI, es porque RTC no necesita electricidad para funcionar. RDSI necesita de una alimentación eléctrica separada.

Ver también: par trenzado (TP), POTS, RDSI, RJ-11.

REPETIDOR

Un repetidor es un dispositivo sencillo que regenera una señal que pasa a través de la red, de tal modo que se puede extender la distancia de transmisión de dicha señal. Un repetidor multipuerto se conoce como un concentrador.

Cuanto más lejos viajan los datos en una red, más débil se hace la señal que lleva ese paquete de datos. Los repetidores *repiten* (regeneran) paquetes de datos, y de este modo, ni el número de paquetes que pasan a través de dichos repetidores, ni la distancia que viajan tienen efecto alguno en la calidad de la señal.

Los repetidores se utilizan también para conectar dos LANs del mismo tipo de red (por ejemplo Ethernet a Ethernet) y trabajan en la capa 1 del modelo de referencia OSI.

Ver también: bridge, capa1, concentrador, LAN, modelo de referencia OSI, red.

RJ-11

Conector estándar utilizado para conectar dispositivos analógicos a una línea telefónica. "RJ" son las siglas de las palabras "registered jack" o clavija registrada.

Ver también: analógico, RJ-45.

RJ-45

Es un conector estándar que se utiliza para conectar las redes Ethernet. "RJ" son las siglas de las palabras "registered jack" o clavija registrada.

Ver también: Ethernet, red.

RS-232

Ver también: EIA/TIA-232.

S

SEGMENTO

Un segmento es un grupo de dispositivos tales como PCs, servidores o impresoras que están conectados entre sí por componentes de un equipo de red. En los segmentos Ethernet, los ordenadores se pueden conectar entre sí por medio de concentradores, y las señales que se difunden en dicho segmento se oyen en todas las estaciones a él conectadas. Si el segmento está interconectado a otro segmento con un bridge o encaminador, es posible enviar paquetes entre dichos segmentos. Se pueden enviar paquetes entre dos segmentos si están interconectados por medio de un bridge o un encaminador. Los segmentos de red conectados por bridges o encaminadores, forman interconexiones de redes. A los segmentos se les llama a menudo *subredes*.

Ver también: bridge, concentradores, encaminador, Ethernet, interconexión de redes, paquete, PC, red, servidor.

SEMIDÚPLEX

Se utiliza el término *semidúplex* para describir transmisiones de datos que pueden ocurrir en dos direcciones en el mismo enlace de comunicaciones, en una sola dirección a un tiempo. Los concentradores operan solamente en modo semidúplex, a diferencia de los conmutadores que pueden operar en ambos modos, full-dúplex y semidúplex.

Ver también cable dúplex, concentrador, conmutador, full dúplex.

SEÑALES ANALÓGICAS

Datos codificados como una forma de onda continua, para transmitir a través de las líneas telefónicas.

Ver también módem.

SERVICIOS DE TARJETA

Servicios de tarjeta en Windows 95 y Windows 98 facilita la función Plug-and-Play a las tarjetas PCMCIA.

Ver también: PCMCIA.

SERVIDOR

Es un ordenador o dispositivo especializado en una red que comparten usuarios múltiples. Un servidor facilita a los usuarios el acceso a servicios de red compartidos, tales como ficheros del ordenador e impresoras.

Ver también: cliente/servidor, red.

SERVIDOR DE IMPRESIÓN

Los servidores de impresión permiten que una impresora esté situada en una ubicación cualquiera de la red.

Funcionan como el "servidor", recibiendo información y pasándola a la impresora para que se puedan imprimir los jobs.

Ver también: red, servidor.

SLIP

Ver Protocolo de Internet de Línea en Serie.

SNMP

Simple Network Management Protocol. Un protocolo estándar definido en IETF, para el intercambio de información de gestión entre entidades de Internet. SNMP es ahora el estándar de facto para virtualmente toda la gestión LAN. Define el formato de los datos de gestión y el tipo de intercambios que pueden tener lugar entre una estación de gestión y el dispositivo que se va a gestionar en la red.

Ver también: protocolo, TCP/IP.

SPID

ID del perfil del servicio. Si es necesario, su compañía telefónica le puede facilitar este número. Generalmente, si su línea RDSI tiene un solo número de teléfono, o no utiliza el servicio RDSI en Norteamérica, no es necesario un SPID.

Ver también: RDSI.

SPX

Intercambio de paquetes secuenciales. Es un protocolo de comunicaciones desarrollado por Novell para utilizar con NetWare, y que se utiliza para controlar el transporte de mensajes a través de una red.

Ver también: NOS, protocolo.

STP

Par trenzado blindado. Es un sistema de cables que consiste en uno o más pares de cables protegidos, utilizados en una gran variedad de aplicaciones de red. Los cables están revestidos de metal para eliminar las interferencias electromagnéticas (EMI) y son de mejor calidad que UTP (Par Trenzado No Blindado).

Ver también: cables de la categoría 3, cables de la categoría 5, par trenzado, red, UTP.

T

TCP/IP

Protocolo de Control de Transmisión/Protocolo de Internet. Este es el nombre de dos de los protocolos más conocidos desarrollados por el Departamento de Defensa de los Estados Unidos en la década de los años 70, para permitir la comunicación entre el equipo de proveedores diferentes. Originariamente era un estándar de UNIX, pero ahora TCP/IP está soportado en casi todas las plataformas, y es el protocolo de Internet.

IP representa el esquema por el cual dos dispositivos (ambos con direcciones IP) se comunican entre sí. TCP gestiona el flujo de paquetes IP, y garantiza que los paquetes están libres de errores y llegan a su destino correctamente.

Ver también: interconexión de redes, Internet, IP, nodos, paquete, protocolo, red, UNIX.

TIA

Asociación de la Industria de la Telecomunicación. Es una organización de estándares de telecomunicación fundada en América en 1988. La TIA se formó por un grupo derivado de la EIA (Asociación de las Industrias Electrónicas) con el fin de definir unos estándares de telecomunicaciones globales, como por ejemplo el EIA/TIA-232.

Ver también: EIA, EIA/TIA-232.

Token Ring

Desarrollado por IBM, Token Ring ofrece un método para conectar dispositivos en una LAN (red de área local). Por ello, Token Ring ofrece el mismo servicio que Ethernet, pero llevado a cabo de un modo diferente: una señal electrónica (un paquete de datos) se pasa a través de estaciones en un anillo. La mayoría de los negocios pequeños instalan redes Ethernet, porque en comparación, son más sencillas que Token Ring.

Las redes Token Ring se asemejan físicamente a la forma de una estrella, pero en realidad actúan como un anillo lógico. Un dispositivo (como un PC) toma la señal, transmite sus datos, y libera la señal después de que los datos han completado el circuito del anillo eléctrico.

El estándar IEEE 802.5 especifica el cableado en el que opera el Token Ring (STP, UTP o cable de fibra óptica); Token Ring opera a 4 o a 16Mbps.

Ver también: cable de fibra óptica, Ethernet, IEEE, LAN, Mbps, paquete, PC, red, STP, UTP.

TRÁFICO

Movimiento de paquetes de datos en una red.

Ver también: paquete, red.

TRAMA

Conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado.

Desde uno de los componentes de equipo de red, los cuadros pueden ser unidestinados (enviados a un solo dispositivo), multidestinados (enviados a dispositivos múltiples) o difundidos (enviados a todos los dispositivos).

Ver también: difusión, multicast, paquete, unicast.

TRANSCCEPTOR

Es un dispositivo que emite y recibe señales digitales y analógicas. En las redes, un transceptor es un dispositivo que conecta una interfaz a una red de área local (LAN). Los transceptores pueden ser unidades independientes, o pueden estar incorporados en una placa de circuito dentro de un ordenador. Se utilizan generalmente para conectar elementos de diferente tipo, como por ejemplo, cable coaxial grueso a un AUI.

Ver también: 10 BASE 5, AUI, cable coaxial, colisión, Ethernet, LAN, red, tráfico.

U

UNIX

Es un sistema operativo desarrollado en 1969 en Bell Laboratories. UNIX es un sistema operativo que puede funcionar en una gran variedad de hardware.

USB

Bus de Serie Universal USB es un nuevo tipo de dispositivo de conexión, instalado en la mayoría de PCs de hoy en día. Facilita un modo de conectar periféricos, como pueden ser una impresora, un ratón, o una cámara digital, a un PC host o anfitrión. Sus principales ventajas son:

1. Reduce la necesidad de instalar tarjetas en ranuras de ordenador dedicadas y tener que reconfigurar el sistema.
2. Ofrece una verdadera instalación plug and play y una gran capacidad de intercambio de dispositivos, gracias a la cual se pueden añadir, quitar o cambiar dispositivos mientras su PC sigue funcionando.

Los puertos USB vienen de fábrica en la mayoría de PCs de sobremesa. Compruebe la parte trasera de su PC y busque el logo USB oficial, o póngase en contacto con el fabricante del PC para averiguar si su ordenador tiene un puerto USB.

USB Concentrador

Concentrador de **Bus de Serie Universal**. Un Hub USB facilita un método de conectar múltiples periféricos USB, como pueden ser una impresora, un ratón, o una cámara digital, a un PC. No puede conectar PCs entre sí.

Ver también: [concentrador](#), [USB](#), [USB Interfaz de red](#).

USB interfaz de red

Interfaz de **Red de Bus de Serie Universal**. La Interfaz de red USB facilita el enlace entre un puerto USB de un PC y una red Ethernet. Ejecuta la misma función que una tarjeta de interfaz de red (NIC) estándar, sin la necesidad de abrir el PC para instalar la tarjeta.

Otra diferencia clave entre la Interfaz de red USB y una NIC convencional es la velocidad de transmisión. Las tarjetas NIC se pueden adquirir en las variedades 10Mbps o 10/100Mbps, y facilitan las conexiones más rápidas entre el PC y la red. La Interfaz de red USB, debido a las limitaciones de velocidad de la tecnología USB, solamente puede adquirirse con una conexión 10Mbps Ethernet.

Ver también: [Ethernet](#), [Mbps](#), [NIC](#), [USB](#).

UTILIZACIÓN DE RED

Es la cantidad de tráfico presente en una red como porcentaje del ancho de banda de la red. La utilización indica cuánta capacidad de la red se está utilizando.

Ver también: [ancho de banda](#), [red](#).

UTP

Par trenzado no blindado. Cable que consiste en un par o más de cables (que se utilizan en una gran variedad de aplicaciones de red) que están enfundados en plástico. UTP es popular porque es muy maleable y no ocupa tanto espacio como los STP y otros cables.

Ver también: [par trenzado](#), [red](#), [STP](#).

V

V.34

Estándar ITU que permite actualmente velocidades de transferencia de datos de hasta 28.000 bps.

Ver también: [bps](#), [ITU](#).

V.34+

Mejora del V.34, que permite velocidades de transferencia de datos de hasta 33.600 bps.

Ver también: [bps](#), [ITU](#), [V.34](#).

V.90

Estándar ITU, que permite a los módems recibir datos a una velocidad de hasta 56 Kbps a través de una red telefónica conmutada pública estándar.

Ver también: [56K](#), [Kbps](#), [ITU](#).

VELOCIDAD DE CABLE

(wire speed) La velocidad de hilo se refiere a la máxima capacidad de conexión. En las conexiones de Ethernet y Fast Ethernet, se define normalmente por la máxima cantidad de paquetes que se pueden transmitir durante una conexión. La velocidad de cable de Ethernet es de 14.880 paquetes por segundo, y la velocidad del hilo de Fast Ethernet es de 148.809 paquetes por segundo.

Ver también: [bit](#), [Ethernet](#), [Fast Ethernet](#), [paquete](#).

VELOCIDAD DE TRANSFERENCIA DE BITS

Es la velocidad a la que se transmiten los bits; se mide habitualmente en bits por segundo (bps).

Ver también: [bps](#), [bit](#).

VPN

Red Privada Virtual. Una red virtual privada (VPN) es una red segura de datos privada establecida a través de Internet, por medio de la cual se reduce en gran medida la cuenta telefónica, porque se accede a ella marcando un número local de tarifa gratis. Utilizando el backbone principal de Internet se necesita hacer una menor inversión en infraestructura de red privada.

Ver también: [principal](#), [Internet](#), [PPTP](#), [red](#).

W

WAN

Red de Área Extensa. Red de comunicaciones que cubre una gran área. Una red WAN puede abarcar una gran área geográfica y puede contener varias redes LAN. La verdadera definición de una red WAN es la de una red que utiliza la red telefónica principal para conectar sus partes, pero más generalmente, se utiliza para describir una red que engloba un área muy extensa.

Ver también: [LAN](#), [red](#) .

WWW

World Wide Web (o *Web*) es un servicio de internet que permite acceder fácilmente a la información en servidores por todo el mundo. Los *navegadores* de Web, tales como Netscape Navigator e Internet Explorer, permiten a los usuarios "navegar la Web" para acceder a esta información. Los documentos WWW se estructuran utilizando HTML (**H**yper**T**ext **M**ark-up **L**anguage) y pueden incorporar aplicaciones JAVA y Javascript.

Ver también: [Hipertexto](#), [HTML](#), [Internet](#), [servidor](#).

X

xDSL

x Línea Subscriptora Digital. Se refiere a las diferentes variaciones de DSL, como por ejemplo ADSL.

Ver también: [ADSL](#), [DSL](#).

XNS

Servicios de red de Xerox. Es un protocolo de red antiguo desarrollado por Xerox, que permite a los usuarios (por ejemplo, a alguien que trabaje con un PC) utilizar ficheros que se encuentran en otro ordenador.

Ver también: [red](#), [PC](#), [protocolo](#).

17. - BIBLIOGRAFIA.-

TELEINFORMATICA Y REDES DE COMPUTADORES

Serie: mundo electrónico.

Autor: Antonio Alabau Muñuz y Juan Riera Garcia

Publicaciones Marcombo.

2 da. Edición

351 Págs.

INFORMATICA PRESENTE Y FUTURO

Autor: Donald h. Sanders

Editorial Mc Graw Hill

3 ra. Edición

887 Págs.

REDES LOCALES DE COMPUTADORAS

Autor: José Beltrao Moura, Jacques Philippe Sauve y William Ferreira Giozza.

Editorial Mc Graw Hill

2 da. Edición

442 Págs..

COMUNICACIÓN DE DATOS, REDES DE COMPUTADORAS Y SISTEMAS ABIERTOS.

Autor: Fred Halsall

Editorial Pearson Educación

4 ta. Edición

951 Págs..

REDES DE COMPUTADORAS

Autor: Andrew S. Tanenbaum

Editorial Prentice Hall

3 ra. Edición

812 Págs..

REDES PARA TODOS

Autor: Mark Gibbs

Editorial Prentice Hall

2 da. Edición

472 Págs..

TECNOLOGIAS EMERGENTES PARA REDES DE COMPUTADORAS.

Autor: Uyles Black
Editorial Pearson Educación
2 da. Edición
459 Págs.

TELEINFORMATICA.

Autor: Rafael Ale y Fernando Cuellar.
Editorial Mc Graw Hill
1 da. Edición
245 Págs.

Paginas en Internet Consultadas

<http://usuarios.tripod.es/gratis/>

<http://www.microsoft.com/latam>

www.lostutoriales.com

www.red.com.mx

www.cabletron.com

www.avaya.com

www.redmexicana.com

www.sisco.com

www.construccionesred.com

www.monografias.com

www.ethek.com

www.geocities.com

www.itesm.com.mx

Entre otras páginas personales de Internet y proveedores de servicios de red.

Publicaciones mensuales.

PC MAGAZINE
Editorial Televisa.

REVISTA RED

SMART BUSSINESS

PC WORLD

PC SEMANAL.

PUBLICACIONES DEL IEEE (SPECTRUM, NETWORK 'S, ETC.)

APUNTES PERSONALES DE VARIOS SEMINARIOS Y CERTIFICACIONES:

SEMINARIO: SEGURIDAD EN REDES
EDITORIAL GRUPO RED.

SEMINARIO: REDES PRIVADAS VIRTUALES MICROSOFT (**VPN**).
EDITORIAL GRUPO RED.

CERTIFICACION HUB SWITCHES CNET
MEXMAL QUERETARO QRO

CERTIFICACION NORTON SYSTEM WORKS 2001.
IMGRAM DICOM LEON GTO.