

REPOSITORIO ACADÉMICO DIGITAL INSTITUCIONAL

Redes ligeras, solución para pequeñas y medianas empresas

Autor: Maria Eugenia Becerril Mungia

**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.





LICENCIATURA EN SISTEMAS COMPUTARIZADOS



TEMA:

REDES LIGERAS

SOLUCIÓN PARA PEQUEÑAS Y MEDIANAS EMPRESAS

POR:

MARIA EUGENIA BECERRIL MUNGUÍA

ASESOR:

ING. SERGIO FRANCISCO BARRAZA IBARRA



**MORELIA, MICHOACÁN
MAYO DE 2004**

Dedicatorias

A Dios, quién ha guiado mis pasos hacia la superación, ayudándome a encontrar la fuerza necesaria para cumplir esta meta.

A mis padres, Rafael Becerril Zendejas y Ma. Eugenia Murguía Alvarez, quienes con su apoyo incondicional y su infinito amor, hicieron posible uno de mis grandes anhelos.

A mi hermano Rafael Isaías, quien a pesar de ya no estar conmigo, me cuida desde donde se encuentra y me ha inspirado para seguir siempre adelante sin importa lo difícil que sea el camino.

A mi hermana Areli, por su cariño, paciencia y consejos que me ayudaron en los momentos difíciles que he pasado durante mi vida.

A mi mejor amigo, Julio Winfred Gil Campuzano, quién en todo momento enalteció el valor de la amistad, siendo un pilar fundamental para el logro de mis objetivos.

A mi asesor, Ing. Sergio Francisco Barraza, cuya colaboración y apoyo fueron decisivos para la culminación de este trabajo.

A mi amiga Miledi, a Rogelio, Alicia, Katia y Jessica, quienes fueron parte importante en mi formación profesional, ocupando un lugar muy especial en mi corazón.

A mi familia que me ha apoyado y ayudado a levantarme cuando he tenido tropiezos en el camino.

Indice.

INTRODUCCIÓN	1
ANTECEDENTES	2
OBJETIVO GENERAL	2
OBJETIVOS PARTICULARES	2
TOPOLOGIAS DE RED	3
ARQUITECTURA CLIENTE – SERVIDOR	7
EL MODELO OSI	9
MEDIOS DE TRANSMISIÓN	15
ESTANDARES PARA REDES DE IEEE	22
REDES BASADAS EN SERVIDORES	23
DISPOSITIVOS DE RED	25
PROTOCOLOS DE RED	27
DIRECCIONES IP Y MASCARAS DE RED	32
CONFIGURACIÓN DE UNA RED "PEER TO PEER" O MULTIPUNTO	33
CONFIGURACIÓN DEL SISTEMA	34
CASO PRACTICO I. SECRETARIA DE SALUD	44
CASO PRACTICO II. UNIDAD DE PROTECCIÓN SOCIAL EN SALUD	59
CONCLUSIONES Y RECOMENDACIONES	62
BIBLIOGRAFÍA	64
GLOSARIO DE TERMINOS	65

Wireless Terminals and
Information Appliances
(Wireless LANs, Tablets and PDA's)

Web
Computing

Cross Platform
Desktops

Remote
Computing

Branch Offices

Terminals
and
Appliances



INTRODUCCIÓN

En la actualidad toda empresa requiere de una herramienta tan indispensable como es la computadora, así mismo un conjunto de ellas para agilizar y controlar la información necesaria, esto significa un ahorro muy considerable, ya que se requiere de menos personal y hay mejor fiabilidad en la información transmitida si se hace un diseño de red confiable, ya que una red no es solamente el tender cables para poder conectar los equipos, sino que se requiere de conocimientos mas profundos e indispensables que el solo saber ponchar un cable.

Cada vez es más difícil la estabilidad económica en una empresa, es por eso que las "Redes Ligeras", son una buena opción, ya que son la mejor alternativa para las pequeñas y medianas empresas. Consiste en la configuración de una red conformada de equipos de características regulares, que aunque no sean tan sofisticadas, cuentan con capacidades que se aprovechan bien en un pequeño laboratorio de cómputo.

En la configuración de una Red Ligera, se nota el ahorro en costos, tiempo, espacio, de igual forma se le pueden agregar impresoras, scanners, fax, modems, reproductor de cd's, quemador, etc. por estar diseñadas para compartir los recursos individuales de cada estación para con las otras computadoras que están conectadas a la red LAN, también podemos controlar el acceso de los mismos recursos asignando privilegios a cada usuario en vez de compartirlo a todos.

El estudio de redes de cómputo comprende un campo bastante amplio, ya que enfatizar en un todo lo correspondiente a la parte de redes de computadores 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 abarcará en la parte teórica los aspectos más importantes de la tecnología actual en diseño e implementación de redes.

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

Las redes tienden a crecer e innovarse, al principio se conectan unas cuantas personas y luego todo el mundo desea conectarse, para disfrutar de los beneficios y servicios que conlleva el hacerlo, tales como correo electrónico, acceso a la información de cualquier tema (Internet), compartir sus archivos, impresoras, comunicarse en línea, etc.

Este documento pretende ser una guía para el instalador de una red ligera, ya que incluye los conceptos básicos e indispensables para comprender como funcionan internamente estas comunicaciones, además que contiene dos ejemplos prácticos de una instalación de red, tanto con servidor como sin él.

ANTECEDENTES.

Las necesidades de compartir recursos e información han obligado a la creación de redes de equipos de computo, mediante la conexión de 2 o más equipos, los usuarios de la red pueden compartir sus archivos y recursos que tienen disponibles en su equipo local a otros usuarios, para así, reducir y hacer eficientes las inversiones de medios de comunicación y transmisión de la información.

Los equipos que comúnmente se comparten son : Impresoras, unidades de CD, disco duro, etc, y los tipos de archivos que utilizan varios usuarios son: archivos de música, videos, procesador de palabras, hojas de calculo, presentaciones y bases de datos, también una red puede servir para compartir el acceso al internet o en casos cada vez mas comunes conectar redes locales distantes entre si, por ejemplo: podemos conectar una red de una empresa en un edificio X, con cada una de sus sucursales, para poder obtener la información de una forma rápida y eficaz.

Las redes pueden ser de muchos tipos, locales, de área amplia, de área metropolitana, etc, conectadas mediante diversos medios de transmisión como alámbricos, inalámbricos, fibra de vidrio, etc, y comunicados también mediante una gran variedad de protocolos, Así que cuando hablamos de redes, solamente podemos dar por sentado que cumplan su finalidad, compartir información y recursos, porque dependerá de las necesidades y posibilidades económicas de cada empresa o lugar para establecer la configuración de red que para ellos sea mejor.

En el caso particular de este trabajo, describimos redes y sus componentes en general, solamente se hace hincapié en las redes ligeras, las cuales son económicas y para contemplarse dentro de esta clasificación se toma en cuenta el tráfico que circula en dicha red.

OBJETIVO GENERAL

Conocer y comprender el funcionamiento, integración, diseño y valoración de una red de equipos de cómputo, así como los dispositivos de red necesarios, medios de transmisión, protocolos y configuraciones para su implementación en un caso real.

OBJETIVOS PARTICULARES

- Identificar los elementos básicos para la instalación de una red.
- Conocer los dispositivos de red especializados.
- Conocer las ventajas y desventajas de una red.
- Identificar los protocolos utilizados en las redes.
- Compartir los recursos.

- Asignar privilegios de acceso.
- Configurar redes con y sin servidor.
- Establecer la seguridad en la red.

TOPOLOGÍAS DE RED.

Las redes de ordenadores surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos.

Los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de **topología de la red**. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

1. La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.
2. La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

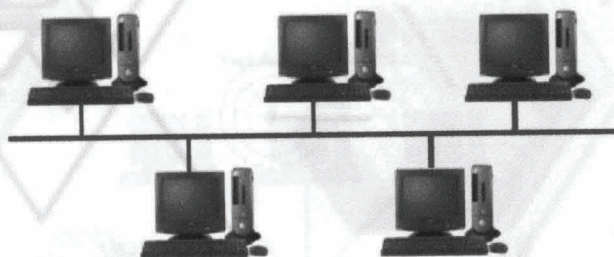
En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

Las principales modelos de topología son:

Topología de bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los host queden desconectados.

Topología de bus



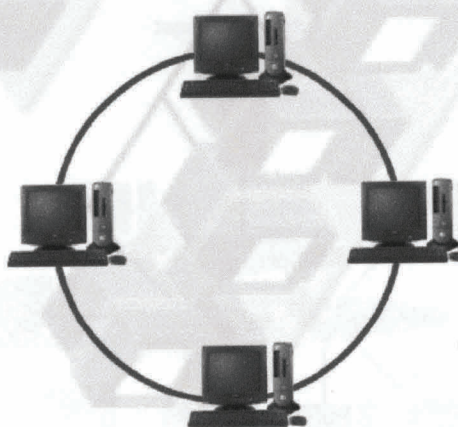
La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes.

Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

Topología de anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

Topología en anillo

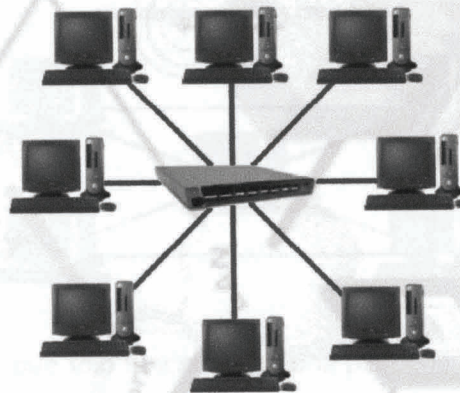


Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

Topología en estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub o switch, pasa toda la información que circula por la red.

Topología en estrella



La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente.

Topología en árbol

La topología en árbol es similar a la topología en estrella, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

Topología en árbol

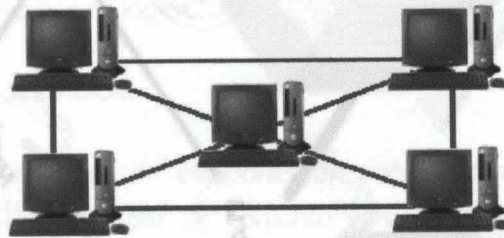


El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

Topología en malla completa

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada nodo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

Topología en malla completa

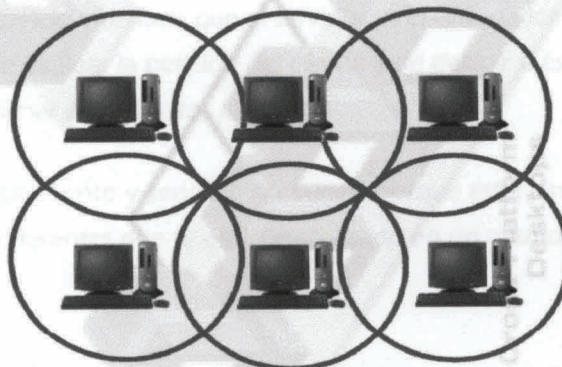


La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

Topología de red celular

La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

Topología de red celular



La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Las topologías LAN más comunes son:

- **Ethernet:** topología de bus lógica y en estrella física.
- **Token Ring:** topología de anillo lógica y una topología física en estrella.
- **FDDI:** topología de anillo física y lógica.

ARQUITECTURA CLIENTE – SERVIDOR.

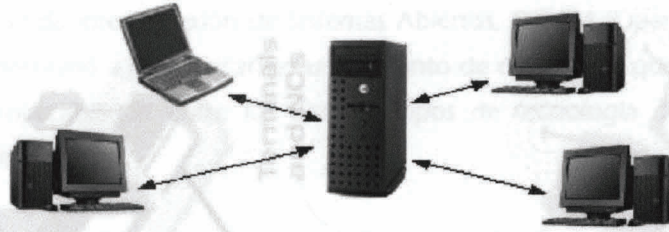
Una red está formada por una serie de estaciones de trabajo, coordinadas por unas máquinas especiales, denominadas servidores, y por un conjunto variable de dispositivos autónomos, como impresoras, escáneres, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs. Cada dispositivo activo que interviene en la comunicación de forma autónoma se denomina nodo.

Todos ellos se comunican entre sí directamente por medios de transmisión físicos (cables coaxiales, de par trenzado o de fibra óptica) o basados en ondas (redes inalámbricas), aunque si el tamaño de la red lo exige pueden hacerlo mediante líneas telefónicas, de radio de largo alcance o por satélite.

Los sistemas de comunicación en red se basan en la *arquitectura cliente-servidor*, que es una forma específica de diseño de aplicaciones, aunque también se conoce con este nombre a los ordenadores en los que estas aplicaciones se están ejecutando. Así, el cliente es el ordenador que se encarga de efectuar una petición o solicitar un servicio, mientras que el servidor es el ordenador remoto que controla dichos servicios y que se encarga de evaluar la petición del cliente y de decidir si ésta es aceptada o rechazada, y si es aceptada, de proporcionar dichos datos al cliente.

Hay que tener en cuenta que cliente y servidor no tienen porque estar en ordenadores separados, ya que pueden ser programas diferentes que se están ejecutando en un mismo computador.

Arquitectura cliente-servidor



A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas, etc. Esta comunicación de datos se realiza mediante el envío de unidades de información, lógicamente agrupadas, denominadas **paquetes de datos**.

Los paquetes de datos incluyen la información origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los dispositivos destino. La dirección origen de un paquete especifica la identidad del computador que envía el paquete. La dirección destino especifica la identidad del computador que finalmente recibe el paquete.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o **protocolo**. Un protocolo es una descripción formal de un conjunto de normas y convenciones que determinan el formato y la transmisión de los datos entre los diferentes dispositivos de una red.

Todo protocolo debe definir los siguientes aspectos en la comunicación de datos:

- **Sintaxis:** el formato de los datos y los niveles de la señal.
- **Semántica:** información de control para la coordinación y el manejo de errores.
- **Temporización:** sincronización de velocidades de secuenciación.

Otro concepto importante es el de **interfaz**, aunque puede resultar complicado de explicar, ya que admite varias definiciones:

- Una interfaz entre equipos es el mecanismo encargado de la conexión física entre ellos, definiendo las normas para las características eléctricas y mecánicas de la conexión.
- Una interfaz entre capas es el mecanismo que hace posible la comunicación entre dichas capas, de forma independiente a las mismas (según esto, entre cada dos capas del modelo OSI habrá una interfaz de comunicación).
- Y a todos nos suena el concepto de interfaz de usuario, que en cualquier aplicación es el sistema por el cual ésta se comunica con el usuario e interactúa con él.

EL MODELO OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, OSI-RM (Open System Interconnection-Reference Model) proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO dividió el modelo de referencia OSI en capas, entendiéndose por **capa** una entidad que realiza de por sí una función específica.

Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

En el modelo de referencia OSI hay siete capas numeradas, cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

1. Divide la comunicación de red en partes más pequeñas y sencillas.
2. Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
3. Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida. Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
4. Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Las siete capas OSI son:

7.	Aplicación
6.	Presentación
5.	Sesión
4.	Transporte
3.	Red
2.	Enlace Datos
1.	Física

Capa 7: La capa de aplicación.

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos de las aplicaciones de usuario acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa 6: La capa de presentación.

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.

Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.

Es también la responsable de la obtención y de liberar la conexión de sesión cuando existan varias alternativas disponibles.

Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.

- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Dar formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos cuando sea necesario.

Capa 5: La capa de sesión.

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos host (máquinas en red) que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin pérdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, chequeando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.
- Sincronizar el diálogo entre las capas de presentación de los dos host y administrar su intercambio de datos, estableciendo las reglas o protocolos para el diálogo entre máquinas, regulando quien habla y por cuanto tiempo.
- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar **tokens**. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación, base de ciertos tipos de redes, como Token Ring o FDDI.
- Hacer **checkpoints**, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

Capa 4: La capa de transporte.

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión.

Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas **segmentos**, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

La capa de transporte intenta suministrar un servicio de transporte de datos que aisle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte confiable de datos entre los nodos de la red.

Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Se conocen con el nombre de **circuitos virtuales** a las conexiones que se establecen dentro de una red. En ellos no hay la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.

Podemos resumir las funciones de la capa de transporte en los siguientes puntos:

- Controlar la interacción entre procesos usuarios en las máquinas que se comunican.
- Incluir controles de integración entre usuarios de la red para prevenir pérdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y el direccionamiento de procesos de máquina a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte confiable, llamadas segmentos, que pasa luego a la capa de red para su envío.
- Realizar funciones de control y numeración de las unidades de información (los segmentos).
- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.
- Garantizar la transferencia de información a través de la red.

Capa 3: La capa de red.

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

Sus principales funciones son:

- Dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas **paquetes**, a los que asigna las direcciones lógicas de los host que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Encaminar la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Ensamblar los paquetes en el host destino.

En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

Capa 2: La capa de enlace.

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo, realizando para ello las siguientes funciones:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agregar una secuencia especial de bits al principio y al final de los paquetes de datos, estructurando este flujo bajo un formato predefinido, denominado **trama**, que suele ser de unos cientos de bytes.
- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.

- Controlar la congestión de la red.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Encargarse del acceso de los datos al medio (soportes físicos de la red).

Capa 1: La capa física.

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

Sus principales funciones las podemos resumir en:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar voltajes y pulsos eléctricos.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

Esta capa solamente reconoce bits individuales.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como **comunicaciones de par-a-par**. Las reglas y convenciones que controlan esta conversación se denominan **protocolo de la capa n**, y se ocupan del formato y significado de las unidades de datos intercambiadas.

Durante este proceso, cada protocolo de capa intercambia unidades de información entre capas iguales de las máquinas que se están comunicando, conocidas con el nombre de **unidades de datos de protocolo (PDU)**. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.



Tipos de Servicios de Red.

También cada capa de un modelo o arquitectura de red recibe servicios a la capa que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario. Hay dos tipos principales de servicios:

1. **Servicios orientados a la conexión:** En ellos la conexión es como un tubo a través del cual se envía la información de forma continua, por lo que los mensajes llegan en el orden que fueron enviados y sin errores. Proporcionan un servicio confiable de comunicación de datos. Una analogía es el sistema telefónico.
2. **Servicios sin conexión:** En los que cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continua y el ruteo de cada mensaje es independiente. El servicio no es entonces confiable, pues la capa de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

Otra clasificación posible de los servicios en la que distingue entre confiables y no confiables:

- **Servicios confiables:** son aquellos en los que la transmisión de datos está controlada en cada momento, pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos. Para ello la máquina receptora envía mensajes de acuse de recibo de las tramas recibidas a la máquina emisora.
- **Servicios no confiables:** en estos no existe un control de los datos transmitidos, por lo que no se puede garantizar que se hayan recibido todos los datos. Una forma de contrarrestar esta debilidad es la implementación de un sistema de acuse de recibo de las unidades de datos.

En realidad, una capa de una máquina no puede transferir los datos de forma directa a su capa par de otra, si no que necesita los servicios de todas las capas que se encuentran por debajo de ella en la jerarquía de capas, pasándose la información hacia abajo hasta llegar al nivel físico, que es el que realiza el proceso de transferencia de datos.

MEDIOS DE TRANSMISIÓN.

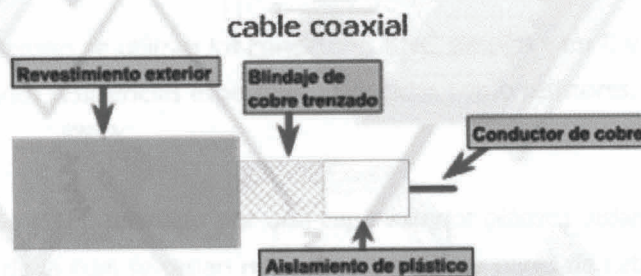
Una vez creadas las señales que nos van a permitir la transmisión de la información, es necesario un puente, un medio físico por el que dichas señales se desplacen desde el host emisor al host destino. Este medio físico puede ser de diferente naturaleza, y la red resultante se clasificará de acuerdo con él.

Los tipos principales de medios físicos son el cableado de cobre, el cableado de fibra óptica y la propia atmósfera, usada en transmisiones sin cable, mediante radiofrecuencias, satélites, etc. Generalmente, en redes LAN, se usa cableado de cobre, en sus diferentes modalidades, para la unión de host generales, reservándose el uso de cableado de fibra óptica para la unión de nodos principales (backbone).

Cableado de cobre.-

El cableado de cobre es, como hemos dicho, el medio más común de unión entre host y dispositivos en redes locales. Los principales tipos de cables de cobre usados son:

1. **Cable Coaxial:** compuesto por un conductor cilíndrico externo hueco que rodea un solo alambre interno compuesto de dos elementos conductores. Uno de estos elementos (ubicado en el centro del cable) es un conductor de cobre. Está rodeado por una capa de aislamiento flexible. Sobre este material aislador hay una malla de cobre tejida o una hoja metálica que actúa como segundo alambre del circuito, y como blindaje del conductor interno. Esta segunda capa de blindaje ayuda a reducir la cantidad de interferencia externa, y se encuentra recubierto por la envoltura plástica externa del cable.



Para las LAN, el cable coaxial ofrece varias ventajas. Se pueden realizar tendidos entre nodos de red a mayores distancias que con los cables STP o UTP (unos 500 metros), sin que sea necesario utilizar tantos repetidores. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos.

El cable coaxial viene en distintos tamaños. El cable de mayor diámetro se especificó para su uso como cable de backbone de Ethernet porque históricamente siempre ha tenido mejores características de longitud de transmisión y limitación del ruido. Este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa. Como su apodo lo indica, debido a su diámetro este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. La regla práctica es: cuanto más difícil es instalar los medios de red, más cara resulta la instalación. El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet no se usa casi nunca, salvo en instalaciones especiales.

En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet o red barata. Sin embargo, como el cobre exterior o trenzado metálico del cable coaxial comprende la mitad del circuito eléctrico, se debe tener especial cuidado para garantizar su correcta conexión a tierra. Esto se hace asegurándose de que haya una sólida conexión eléctrica en ambos extremos del cable. Sin

embargo, a menudo, los instaladores omiten hacer esto. Como resultado, la mala conexión del blindaje resulta ser una de las fuentes principales de problemas de conexión en la instalación del cable coaxial. Estos problemas producen ruido eléctrico que interfiere con la transmisión de la señal a través de los medios de networking. Es por este motivo que, a pesar de su diámetro pequeño, thinnet ya no se utiliza con tanta frecuencia en las redes Ethernet.

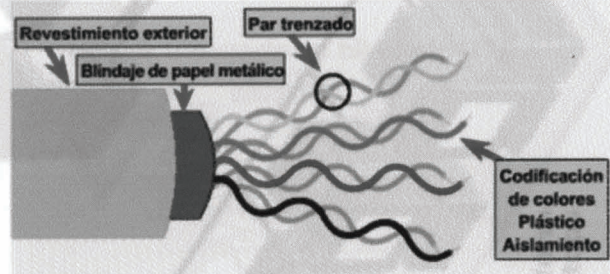
conectores BNC



Para conectar cables coaxiales se utilizan los conectores BNC, simples y en T, y al final del cable principal de red hay que situar unas resistencias especiales, conocidas como resistores, para evitar la reflexión de las ondas de señal.

2. **Par trenzado blindado (STP):** formado por una capa exterior plástica aislante y una capa interior de papel metálico, dentro de la cual se sitúan normalmente cuatro pares de cables, trenzados para a par, con revestimientos plásticos de diferentes colores para su identificación. Combina las técnicas de blindaje, cancelación y trenzado de cables. Según las especificaciones de uso de las instalaciones de red Ethernet, STP proporciona resistencia contra la interferencia electromagnética y de la radiofrecuencia sin aumentar significativamente el peso o tamaño del cable. El cable de par trenzado blindado tiene las mismas ventajas y desventajas que el cable de par trenzado no blindado. STP brinda mayor protección contra todos los tipos de interferencia externa, pero es más caro que el cable de par trenzado no blindado.

par trenzado blindado STP



A diferencia del cable coaxial, el blindaje en el STP no forma parte del circuito de datos y, por lo tanto, el cable debe estar conectado a tierra en ambos extremos. Normalmente, los instaladores conectan STP a tierra en el armario para el cableado y el hub o switch, aunque esto no siempre es fácil de hacer, especialmente si los instaladores intentan usar paneles de conexión antiguos que no fueron diseñados para cable STP. Si la conexión a tierra no está bien realizada, el STP puede transformarse en una fuente de problemas, ya que permite que el blindaje actúe como si fuera una antena, absorbiendo las señales

eléctricas de los demás hilos del cable y de las fuentes de ruido eléctrico que provienen del exterior del cable.

No es posible realizar tendidos de cable STP tan largos como con otros medios de networking (como, por ejemplo, cable coaxial) sin repetir la señal, siendo la longitud máxima de cable recomendada de unos 100 metros, y su rendimiento suele ser de 10-100 Mbps.

Se especifica otro tipo de STP para instalaciones Token Ring. En este tipo de cable, conocido como STP de 150 ohmios, el cable no sólo está totalmente blindado para reducir la interferencia electromagnética y de radiofrecuencia, sino que a su vez cada par de hilos trenzados se encuentra blindado con respecto a los demás para reducir la diafonía. Si bien el blindaje empleado en el cable de par trenzado blindado de 150 ohmios no forma parte del circuito, como sucede con el cable coaxial, aún así debe estar conectado a tierra en ambos extremos. Este tipo de cable STP requiere una cantidad mayor de aislamiento y de blindaje. Estos factores se combinan para aumentar de manera considerable el tamaño, peso y costo del cable. También requiere la instalación de grandes armarios y conductos para el cableado, lujos que en muchos edificios antiguos no pueden permitirse.

Para la conexión de los cables STP a los diferentes dispositivos de red se usan unos conectores específicos, denominados conectores STP, similares a los RJ-45 descritos más abajo.

3. **Par trenzado no blindado (UTP):** compuesto por cuatro pares de hilos, trenzados para a par, y revestidos de un aislante plástico de colores para la identificación de los pares. Cada par de hilos se encuentra aislado de los demás. Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuanto trenzado se permite por unidad de longitud del cable.



Cuando se usa como medio de networking, el cable UTP tiene cuatro pares de hilos de cobre de calibre 22 ó 24. El UTP que se usa como medio de networking tiene una impedancia de 100 ohmios. Esto lo diferencia de los otros tipos de cables de par trenzado, como, por ejemplo, los que se utilizan para los teléfonos. Como el UTP tiene un diámetro externo de aproximadamente 0,43 cm, el hecho de que su

tamaño sea pequeño puede ser ventajoso durante la instalación. Como el UTP se puede usar con la mayoría de las arquitecturas de networking principales, su popularidad va en aumento.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios de networking. De hecho, el cable UTP cuesta menos por metro que cualquier otro tipo de cableado de LAN, sin embargo, la ventaja real es su tamaño. Como su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Este puede ser un factor sumamente importante para tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad.

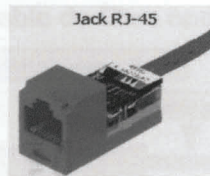
Sin embargo, el cableado de par trenzado también tiene una serie de desventajas. El cable UTP es más sensible al ruido eléctrico y la interferencia que otros tipos de medios de networking. Además, en una época el cable UTP era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable UTP es el más rápido entre los medios basados en cobre.

La distancia máxima recomendada entre repetidores es de 100 metros, y su rendimiento es de 10-100 Mbps.

Para conectar el cable UTP a los distintos dispositivos de red se usan unos conectores especiales, denominados RJ-45 (Registered Jack-45), muy parecidos a los típicos conectores del cableado telefónico casero.



Este conector reduce el ruido, la reflexión y los problemas de estabilidad mecánica y se asemeja al enchufe telefónico, con la diferencia de que tiene ocho conductores en lugar de cuatro. Se considera como un componente de networking pasivo ya que sólo sirve como un camino conductor entre los cuatro pares del cable trenzado de Categoría 5 y las patas de la toma RJ-45. Se considera como un componente de la Capa 1, más que un dispositivo, dado que sirve sólo como camino conductor para bits.



Los enchufes o conectores RJ-45 se insertan en jacks o receptáculos RJ-45. Los jacks RJ-45 tienen 8 conductores, que se ajustan a los del conector RJ-45. En el otro lado del jack RJ-45 hay un bloque de inserción donde los hilos individuales se separan y se introducen en ranuras mediante una herramienta similar a un tenedor denominada herramienta de punción.

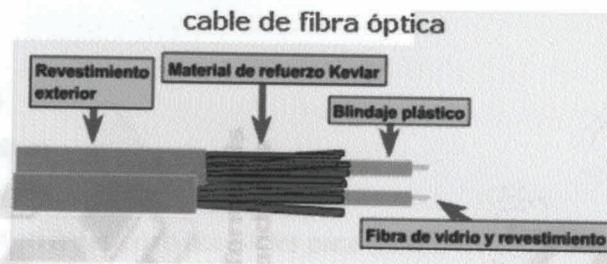
panel de conexión



Para centralizar los diferentes conectores RJ-45 se utilizan unos dispositivos especiales, denominados **paneles de conexión**. Vienen provistos de 12, 24 ó 48 puertos y normalmente están montados en un bastidor. Las partes delanteras son jacks RJ-45; las partes traseras son bloques de punción que proporcionan conectividad o caminos conductores.

4. **Cable de Fibra Óptica:** puede conducir transmisiones de luz moduladas. Si se compara con otros medios de networking, es más caro, sin embargo, no es susceptible a la interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera de los demás tipos de medios de networking descritos aquí. El cable de fibra óptica no transporta impulsos eléctricos, como lo hacen otros tipos de medios de networking que usan cables de cobre. En cambio, las señales que representan a los bits se convierten en haces de luz.

Está compuesto por dos fibras envueltas en revestimientos separados. Si se observa una sección transversal de este cable, veremos que cada fibra óptica se encuentra rodeada por capas de material amortiguador protector, normalmente un material plástico como Kevlar, y un revestimiento externo. El revestimiento exterior protege a todo el cable. Generalmente es de plástico y cumple con los códigos aplicables de incendio y construcción. El propósito del Kevlar es brindar una mayor amortiguación y protección para las frágiles fibras de vidrio que tienen el diámetro de un cabello. Siempre que los códigos requieran que los cables de fibra óptica deban estar bajo tierra, a veces se incluye un alambre de acero inoxidable como refuerzo.



Las partes que guían la luz en una fibra óptica se denominan núcleo y revestimiento. El núcleo es generalmente un vidrio de alta pureza con un alto índice de refracción. Cuando el vidrio del núcleo está recubierto por una capa de revestimiento de vidrio o de plástico con un índice de refracción bajo, la luz se captura en el núcleo de la fibra. Este proceso se denomina reflexión interna total y permite que la fibra óptica actúe como un "tubo de luz", guiando la luz a través de enormes distancias, incluso dando vuelta en codos.

La longitud máxima de cable recomendada entre nodos es de 2.000 metros, y su rendimiento es alto, de 100 o más Mbps.

Comparativo de Medios Físicos de Transmisión.

	10Base5	10Base2	10BaseT	10BaseFP	100BaseTX	100BaseFX
Cableado	Coaxial		Par trenzado	Par de fibra óptica	Par trenzado	2 fibras ópticas
Velocidad	10 Mbps				100 Mbps	
Topología	Bus			Estrella		
Longitud máxima	500 m	185 m	100 m	500 m	100 m	100 m
Nodos por segmento	100	30	2 (un extremo es el hub y el otro el ordenador)			

5. Medios inalámbricos: se basan en la transmisión de ondas electromagnéticas, que pueden recorrer el vacío del espacio exterior y medios como el aire, por lo que no es necesario un medio físico para las señales inalámbricas, lo que hace que sean un medio muy versátil para el desarrollo de redes.

La aplicación más común de las comunicaciones de datos inalámbricas es la que corresponde a los usuarios móviles, cuyo medio físico de comunicación es el aire.

No pretende reemplazar una red cableada, sólo la complementa en situaciones donde es difícil realizar una conexión.

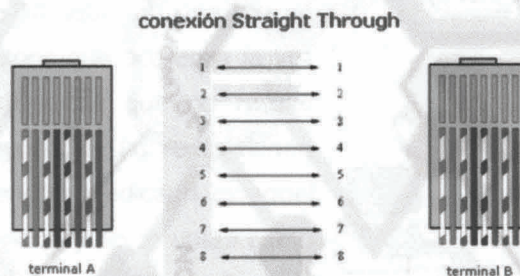
Aplicaciones:

- Expandir una red
- Movilidad de equipos
- Crear una nueva red
- Instalación de red en áreas poco accesibles para cablear
- Colocación de LAN temporal
- Enlace entre edificios

En nuestros estudios de redes LAN Ethernet vamos a centrarnos en el cableado UTP Cat5, que es el comúnmente utilizado.

Configuración del Cable UTP. (Straight Trough)

Este tipo de configuración se usa en cables que van a conectar un host a una red Ethernet 10BaseT. Generalmente, un extremo del cable (terminal A) se conecta al Jack de la tarjeta de red del host, mientras que el otro extremo (terminal B) se conecta a un hub o switch central. El esquema de conexiones es el que sigue:



ESTÁNDARES PARA REDES DE LA IEEE.

El *Instituto de Ingenieros Electrónicos y Eléctricos (IEEE)* es otro organismo que ha procurado normalizar la comunicación entre ordenadores. Este organismo está acreditado por *ANSI*, que es el organismo de estandarización en los EE.UU.

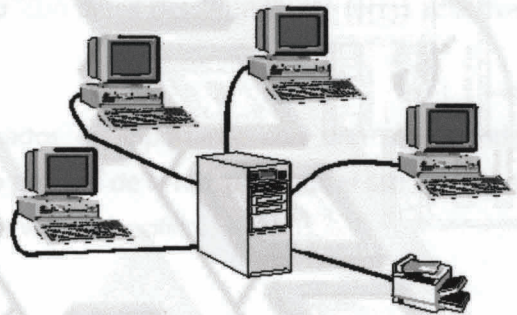
Para ello, propuso la norma 802 que indica que una red local es un sistema de comunicaciones que permite a varios dispositivos comunicarse entre sí. Para ello definieron, entre otros, el tamaño de la red, la velocidad de transmisión, los dispositivos conectados, el reparto de recursos y la fiabilidad de la red que cubren el nivel Físico y el nivel de Enlace de datos (Control de Enlace Lógico y Control de Acceso al Medio). Adicionalmente, el subcomité IEEE 802.1 elabora documentos relativos a la arquitectura de red, interoperación y gestión de red.

Entre las distintas especificaciones de la norma 802 se encuentran:

- IEEE 802.1 (1990). Normalización de la interfaz con Niveles Superiores; se encarga del control de temas comunes: gestión de la red, mensajería, etc.
- IEEE 802.2 (1990). Normalización para el control de Enlace Lógico.
- IEEE 802.3 (1990). Desarrollo de protocolo de Acceso Múltiple con Detección de Portadora y Detección de Colisión.
- IEEE 802.4 (1990). Desarrollo del bus de paso de Testigo.
- IEEE 802.5 (1989-1991). Especificaciones para una configuración de anillo con paso de testigo.
- IEEE 802.6 (1990). Especificaciones para una red de área metropolitana.
- IEEE 802.7. Redes locales de banda ancha.
- IEEE 802.8. Fibra Óptica.
- IEEE 802.9. Estándar para la definición de voz y datos en las redes locales.
- IEEE 802.10. Seguridad en las redes locales.
- IEEE 802.11. Redes locales inalámbricas.

REDES BASADAS EN SERVIDOR.

En un entorno con más de 10 usuarios, una red de Trabajo en Grupo (con equipos que actúen a la vez como servidores y clientes) puede que no resulte adecuada. Por tanto, la mayoría de las redes tienen servidores dedicados. Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación, Los servidores se llaman «dedicados» porque no son a su vez clientes, y porque están optimizados para dar servicio con rapidez a peticiones de clientes de la red, y garantizar la seguridad de los archivos y directorios. Las redes basadas en servidor se han convertido en el modelo estándar para la definición de redes.



A medida que las redes incrementan su tamaño (y el número de equipos conectados y la distancia física y el tráfico entre ellas crece), generalmente se necesita más de un servidor. La división de las tareas de la red entre varios servidores asegura que cada tarea será realizada de la forma más eficiente posible.

Los servidores necesitan realizar tareas complejas y variadas. Los servidores para grandes redes se han especializado para adaptarse a las necesidades de los usuarios. A continuación se dan ejemplos de los diferentes tipos de servidores incluidos en muchas redes de gran tamaño.

Servidores de archivos e impresión: Los servidores de archivos e impresión gestionan el acceso de los usuarios y el uso de recursos de archivos e impresión. Por ejemplo, al ejecutar una aplicación de

tratamiento de textos, la aplicación de tratamiento de textos se ejecuta en su equipo. El documento de tratamiento de textos almacenado en el servidor de archivos e impresión se carga en la memoria de su equipo, de forma que pueda editarlo o modificarlo de forma local. En otras palabras, los servidores de archivos e impresión se, utilizan para el almacenamiento de archivos y datos.

Servidores de aplicaciones: Los servidores de aplicaciones constituyen el lado servidor de las aplicaciones cliente/servidor, así como los datos, disponibles para los clientes. Por ejemplo, los servidores almacenan grandes cantidades de datos organizados para que resulte fácil su recuperación. Por tanto, un servidor de aplicaciones es distinto de un servidor de archivos e impresión. Con un servidor de archivos e impresión, los datos o el archivo son descargados al equipo que hace la petición. En un servidor de aplicaciones, la base de datos permanece en el servidor y sólo se envían los resultados de la petición al equipo que realiza la misma.

Una aplicación cliente que se ejecuta de forma local accede a los datos del servidor de aplicaciones. Por ejemplo, podría consultar la base de datos de empleados buscando los empleados que han nacido en noviembre. En lugar de tener la base de datos completa, sólo se pasará el resultado de la consulta desde el servidor a su equipo local.

Servidores de correo: Los servidores de correo funcionan como servidores de aplicaciones, en el sentido de que son aplicaciones servidor y cliente por separado, con datos descargados de forma selectiva del servidor al cliente.

La planificación para el uso de servidores especializados es importante con una red grande. El planificador debe tener en cuenta cualquier crecimiento previsto de la red, para que el uso de ésta no se vea perjudicado si es necesario cambiar el papel de un servidor específico.

Ventajas de las redes basadas en servidor

Aunque resulta más compleja de instalar, gestionar y configurar, una red basada en servidor tiene muchas ventajas sobre una red simple *Trabajo en Grupo*.

Compartir recursos: Un servidor está diseñado para ofrecer acceso a muchos archivos e impresoras manteniendo el rendimiento y la seguridad de cara al usuario.

El compartir datos basado en servidor puede ser administrado y controlado de forma centralizada. Como estos recursos compartidos están localizados de forma central, son más fáciles de localizar y mantener que los recursos situados en equipos individuales.

Seguridad: La seguridad es a menudo la razón primaria para seleccionar un enfoque basado en servidor en las redes. En un entorno basado en servidor, hay un administrador que define la política y la aplica a todos los usuarios de la red, pudiendo gestionar la seguridad.

Copia de seguridad: Las copias de seguridad pueden ser programadas varias veces al día o una vez a la semana, dependiendo de la importancia y el valor de los datos. Las copias de seguridad del servidor pueden programarse para que se produzcan automáticamente, de acuerdo con una programación determinada, incluso si los servidores están localizados en sitios distintos de la red.

Redundancia: Mediante el uso de métodos de copia de seguridad llamados sistemas de redundancia, los datos de cualquier servidor pueden ser duplicados y mantenidos en línea. Aun en el caso de que ocurran daños en el área primaria de almacenamiento de datos, se puede usar una copia de seguridad de los datos para restaurarlos.

Número de usuarios: Una red basada en servidor puede soportar miles de usuarios. Este tipo de red sería, imposible de gestionar como red Trabajo en Grupo, pero las utilidades actuales de monitorización y gestión de la red hacen posible disponer de una red basada en servidor para grandes cifras de usuarios.

Hardware: El hardware de los equipos cliente puede estar limitado a las necesidades del usuario, ya que los clientes no necesitan la memoria adicional (RAM) y el almacenamiento en disco necesarios para los servicios de servidor.

DISPOSITIVOS DE RED

NIC/MAU (Tarjeta de red)

"Network Interface Card" (Tarjeta de interfaz de red) o "Medium Access Unit" (Medio de unidad de acceso). Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico.

Hubs (Concentradores)

Son equipos que permiten estructurar el cableado de las redes. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc.

Switches

Son dispositivos similares a los concentradores, solo que funcionan de forma más rápida al contar con una topología interna en forma de estrella (los hubs usan la de bus), por lo que no envía los paquetes a todos los host, los identifica mediante su IP para enviar los paquetes solamente al destinatario que corresponde, reduciendo el tráfico en la red y aumentando la velocidad de transmisión.

Repetidores

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con

lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

Bridges (Puentes)

Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

Routers (Encaminadores)

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

Servidores

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios ordenadores multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor.

Módems

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras.

Los módems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

Modem xDSL

Bajo el nombre xDSL se definen una serie de tecnologías que permiten el uso de una línea de cobre (la que conecta nuestro domicilio con la central de Telefónica) para transmisión de datos de alta velocidad y, a la vez, para el uso normal como línea telefónica. Se llaman xDSL ya que los acrónimos de estas tecnologías acaban en DSL, que está por "Digital Subscriber Line" (línea de abonado digital): HDSL, ADSL, RADSL, VDSL. Cada una de estas tecnologías tiene distintas características en cuanto a prestaciones (velocidad de la transmisión de datos) y distancia de la central (ya que el cable de cobre no estaba pensado para eso, a cuanta más distancia peores prestaciones). Entre estas tecnologías la más adecuada para un uso domestico de Internet es la llamada ADSL.

PROCOLOS DE RED.

Un protocolo de red es como un lenguaje para la comunicación de información. Son las reglas y procedimientos que se utilizan en una red para comunicarse entre los nodos que tienen acceso al sistema de cable. Los protocolos gobiernan dos niveles de comunicaciones:

- Los protocolos de alto nivel: Estos definen la forma en que se comunican las aplicaciones.
- Los protocolos de bajo nivel: Estos definen la forma en que se transmiten las señales por cable.

Como es frecuente en el caso de las computadoras el constante cambio, también los protocolos están en continuo cambio. Actualmente, los protocolos más comúnmente utilizados en las redes son Ethernet, Token Ring y ARCNET. Cada uno de estos está diseñado para cierta clase de topología de red y tienen ciertas características estándar.

PPP - Protocolo Punto a Punto

La mayor parte de la infraestructura de redes de área extensa está construida a partir de líneas alquiladas punto a punto.

En la práctica, la comunicación punto a punto se utiliza de diferentes maneras. Actualmente, una de las formas más habituales de conectarse a Internet para un usuario común es a través de un módem y una línea telefónica. En general, la PC llama al *router* de su proveedor de Internet y así actúa como *host* de la Red. Este método de operación no es distinto a tener una línea arrendada entre la PC y el *router*, excepto que la conexión desaparece cuando el usuario termina la sesión.

Tanto para la conexión por línea alquilada de *router* a *router* como para la conexión conmutada de *host* a *router* se requiere de un protocolo punto a punto de enlace de datos en la línea, para el manejo de marcos de control de errores y las demás funciones de la capa de enlace de datos.

Según nos acercamos al medio físico, la diversidad de los mismos provoca que existan varios protocolos a nivel de enlace de datos para adaptarse a las peculiaridades de cada medio físico.

Dos protocolos de este nivel utilizados ampliamente en Internet son SLIP (*Serial Line Internet Protocol*) y PPP (*Point to Point Protocol*).

Si bien el protocolo SLIP está específicamente diseñado para el transporte de tráfico TCP/IP, la tendencia actual es hacia el uso cada vez mayor del protocolo PPP, ya que también es apto para líneas telefónicas conmutadas, siempre que nuestro proveedor de Internet disponga de este protocolo para atender nuestra llamada.

Al utilizar SLIP, es necesario conocer tanto nuestra dirección IP como la de nuestro proveedor, lo que puede causarnos problemas en el caso de que este asigne dinámicamente las direcciones (algo muy común actualmente). Igualmente, existe la posibilidad de tener que configurar algunos parámetros como pueden ser la máxima unidad de transmisión (MTU), máxima unidad de recepción (MRU), el uso de cabeceras de compresión, etc.

El PPP fue desarrollado por el IETF (*Internet Engineering Task Force*) en 1993 para mejorar estas y algunas otras deficiencias, y crear un estándar internacional, por lo cual en este trabajo desarrollaremos principalmente el protocolo PPP, luego de lo que concluiremos con una breve comparación con su par (SLIP).

El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos "pares" (a partir de aquí, y hasta el final de este trabajo, utilizaremos el término "par" para referirnos a cada una de las máquinas en los dos extremos del enlace - en inglés es *peer*).

Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Tiene tres componentes:

1. Un mecanismo de enmarcado para encapsular datagramas multiprotocolo y manejar la detección de errores.
2. Un protocolo de control de enlace (LCP, *Link Control Protocol*) para establecer, configurar y probar la conexión de datos.
3. Una familia de protocolos de control de red (NCPs, *Network Control Protocols*) para establecer y configurar los distintos protocolos de nivel de red.

Funcionamiento general

Para dar un panorama inicial del funcionamiento de este protocolo en el caso comentado, en que un usuario de una PC quiera conectarse temporalmente a Internet, describiremos brevemente los pasos a seguir:

En primera instancia, la PC llama al *router* del ISP (*Internet Service Provider*, proveedor del servicio de Internet), a través de un módem conectado a la línea telefónica.

Una vez que el módem del *router* ha contestado el teléfono y se ha establecido una conexión física, la PC manda al *router* una serie de paquetes LCP en el campo de datos de uno o más marcos PPP (esto será explicado con mayor detalle más adelante). Estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.

Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.

Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.

En este momento la PC ya es un *host* de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP.

Luego se usa LCP para cancelar la conexión de la capa de enlace de datos.

Finalmente la computadora indica al módem que cuelgue el teléfono, liberando la conexión de la capa física.

PPP puede utilizarse no solo a través de líneas telefónicas de discado, sino que también pueden emplearse a través de SONET o de líneas HDLC orientadas a bits.

Configuración básica

Los enlaces PPP son fáciles de configurar. El estándar por defecto maneja todas las configuraciones simples. Se pueden especificar mejoras en la configuración por defecto, las cuales son automáticamente comunicadas al "par" sin la intervención del operador. Finalmente, el operador puede configurar explícitamente las opciones para el enlace, lo cual lo habilita para operar en ambientes donde de otra manera sería imposible.

Esta auto-configuración es implementada a través de un mecanismo de negociación de opciones extensible en el cual cada extremo del enlace describe al otro sus capacidades y requerimientos.

NETBEUI (Microsoft)

Características y las capas del protocolo 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 Pc's 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.

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.

ETHERNET:

- Actualmente es el protocolo más sencillo y es de bajo costo. Utiliza la topología de "Bus" lineal.
- Ethernet es el nombre de una de las redes de área local más populares hoy en día.
- Inventada por Xerox PARC a principios de los 70's. La versión descrita fue estandarizada por Xerox Corporation y Digital Equipment Corporation en 1978.
- IEEE sacó una versión compatible con la norma bajo el número 802.3.
- La tecnología ethernet consiste fundamentalmente en un cable coaxial thick llamado *ether* de aproximadamente ½ pulgada de diámetro y hasta 500 metros de longitud.
- Estos pueden ser extendidos por medio de dispositivos llamados repetidores que duplican señales eléctricas de un cable a otro.
- Solo dos repetidores pueden ser usados entre dos computadoras, por lo que la longitud máxima de un ethernet es bastante moderada (1500 metros).

Protocolos TCP/IP

Protocolos de comunicaciones.

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de máquinas que estén conectadas (PC, Mac, AS-400...).
- Abstracter a los usuarios de los enlaces utilizados (red telefónica, radioenlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de ordenadores, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.

Diferentes empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando diferentes familias de protocolos, y dándoles diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.).

TCP/IP

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras máquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores, además de los que proporciona los protocolos TCP e IP.

Arquitectura de protocolos TCP/IP

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...)
- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen.

Descomposición en niveles de TCP/IP.

Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en subproblemas de más fácil solución.

A diferencia del OSI, formado por una torre de siete niveles, TCP/IP se descompone en cinco niveles, cuatro niveles software y un nivel hardware. Estos niveles de TCP/IP tienen cierto paralelismo con los del modelo OSI.

DIRECCIONES IP Y MÁSCARAS DE RED

En una red TCP/IP los ordenadores se identifican mediante un número que se denomina **dirección IP**. Esta dirección ha de estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece, estos rangos son concedidos por un organismo central de Internet, el NIC (Network Information Center).

Una dirección IP está formada por 32 bits, que se agrupan en octetos:

01000001 00001010 00000010 00000011

Para entendernos mejor utilizamos las direcciones IP en formato decimal, representando el valor decimal de cada octeto y separando con puntos:

129.10.2.3

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha.

CONFIGURACIÓN DE UNA RED "PEER TO PEER" Ó MULTIPUNTO

Conexiones Multipunto

Una red multipunto es aquella en la que todos los equipos se conectan a una línea troncal (común). Cada equipo debe tener un conector que una la línea del equipo con la línea troncal.

En estas conexiones se conectan múltiples dispositivos al enlace que se ramifican desde un único punto. Generalmente, el dispositivo que proporciona la conexión es un controlador inteligente, que manejan el flujo de información de los múltiples dispositivos unidos a ella.

Conexiones Punto a Punto

Es el conjunto de medios que hacen posible la comunicación entre dos puntos determinados, de forma permanente y sin posibilidad de acceder a la red pública telefónica ni a ningún otro circuito, durante las 24 horas del día, sin necesidad de realizar ningún tipo de marcado para establecer la comunicación.

Este tipo de circuitos esta indicado siempre que deseen transmitir grandes volúmenes de datos entre dos puntos a una velocidad de transmisión alta.

Se puede llegar por varios caminos, con lo que se hacen muy importantes las rutinas de enrutamiento o ruteo. Es más frecuente en redes MAN y WAN.

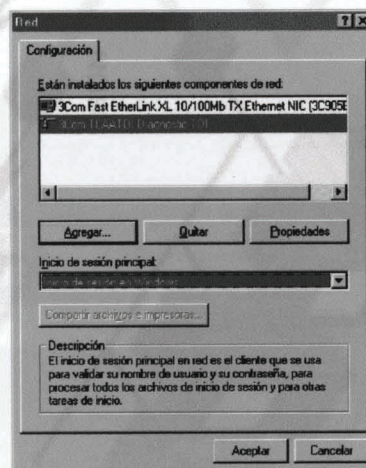
Es una red en la que todos participan de manera activa y comparten recursos (datos, impresoras, periféricos, etc.), sin embargo con un bajo nivel de seguridad, ya que **no existe un servidor** que regule los accesos a los diferentes recursos de la red.

Los sistemas punto a punto permiten que las computadoras sean tanto clientes como servidores al mismo tiempo. Como alternativa, cada computadora puede ser uno o el otro. Si una computadora se convierte en un servidor únicamente, el sistema se comportará como si estuviera basado en un servidor de archivos. Todas las computadoras pueden tener impresoras conectadas a ellas que estén disponibles para todas las demás

Configuración del Sistema bajo Microsoft Windows 98.

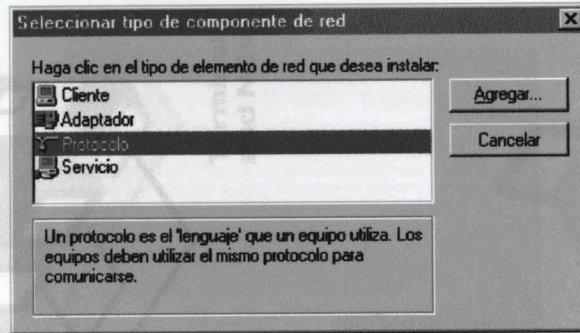
Para configurar nuestro sistema operativo de forma que podamos trabajar en red lo primero desde luego será comprar el cableado necesario e instalar la tarjeta de red. La tarjeta de red se instala como cualquier otra tarjeta que se instale en el ordenador. Si esta es Plug & Play (lo más habitual hoy en 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.

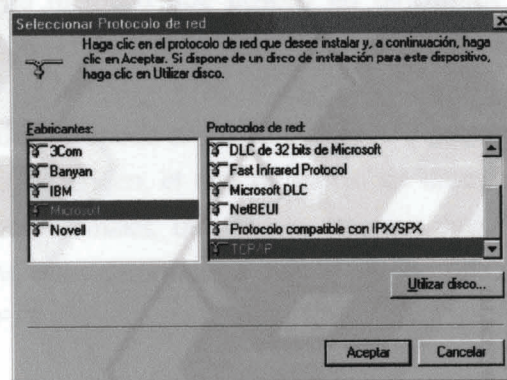


Vemos que aparece la tarjeta de red y debajo un icono con la leyenda "3Com TCAATDI Diagnostic TDI", esto es lo que aparece cuando se instala la tarjeta de red, es decir, todo esto llega aquí automáticamente. ¿Qué es lo que hemos de añadir nosotros?. Para trabajar en red necesitamos en primer lugar una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



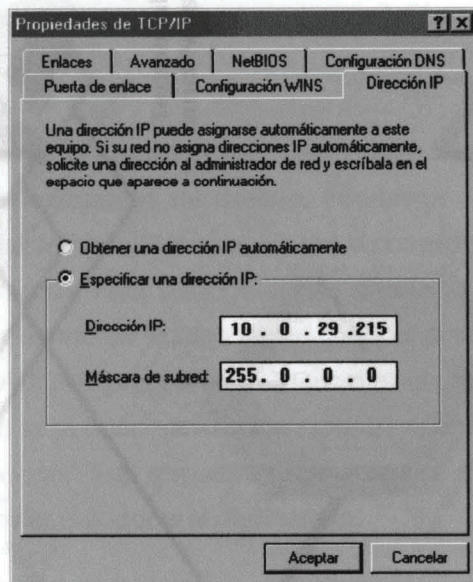
Aparecen cuatro opciones, agregar un cliente, agregar un Adaptador, agregar un Protocolo o agregar un Servicio. Agregar un adaptador instala una nueva tarjeta de red, agregar un protocolo instala un protocolo, lo mismo para servicio. Si agregamos un cliente se instalarán una serie de funciones que el 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 click 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** o también **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 las máscaras 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.

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

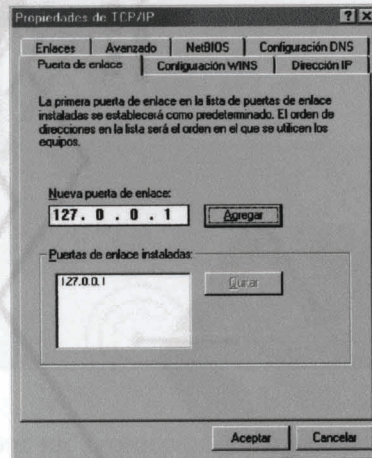
Máscara de subred: 255 . 255 . 0 . 0

Tipo C:

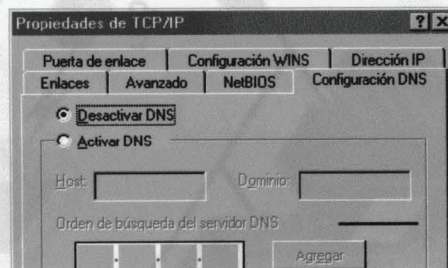
Dirección IP: 192-223 . 0-255 . 0-255 . 0-255

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:

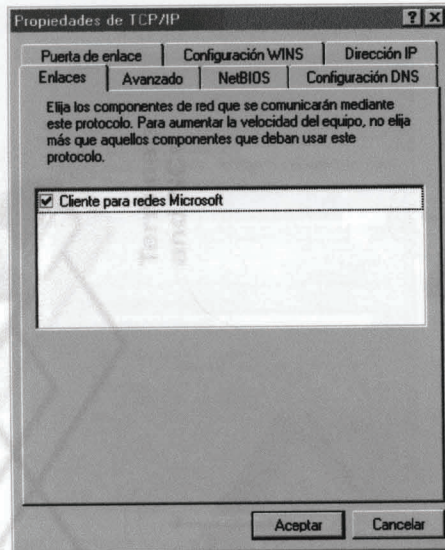


Según lo visto arriba, una dirección IP hace referencia a una red y a un equipo dentro de la red. En nuestro caso estamos en la red 10 y somos el equipo 0.29.25. Si quisieramos conectar con un equipo de la red 11 deberíamos hacerlo a través de una puerta de enlace, esto es, un equipo que está en la red 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.



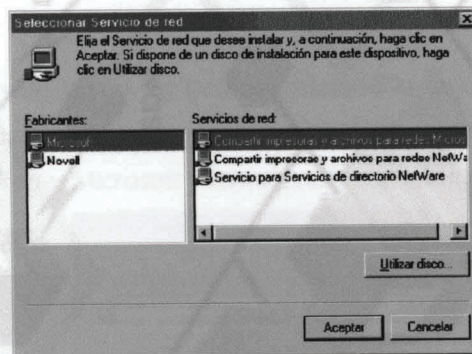
Configuración DNS. DNS es un ordenador en el que se almacena todas las direcciones de los equipos de red. A cada dirección se le asigna un nombre, por ejemplo a nuestra dirección 10.0.29.215 se le asigna el nombre PC_Amigo. Cualquier llamada futura que se quiera hacer a nuestro ordenador se puede hacer 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.

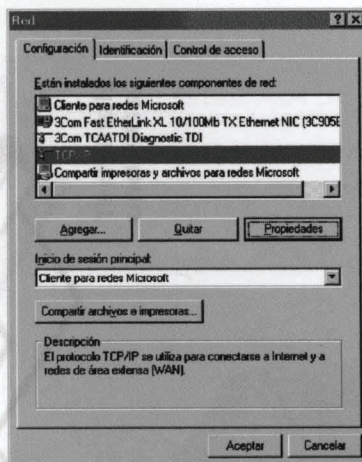


Esta configuración aparece en todos los protocolos. Indica que servicios o clientes van a utilizar este protocolo. En nuestro caso vemos que aparece el único cliente que tenemos instalado. Como era de esperar, teniendo únicamente un protocolo y un cliente, el cliente llevará a cabo sus funciones mediante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

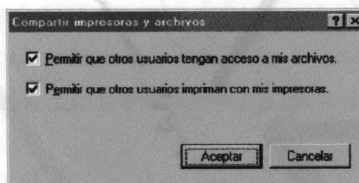
Una vez tenemos instalado el protocolo vamos a añadir un servicio que es la compartición de archivos e impresoras entre ordenadores. Para añadirlo elegimos añadir servicio...



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



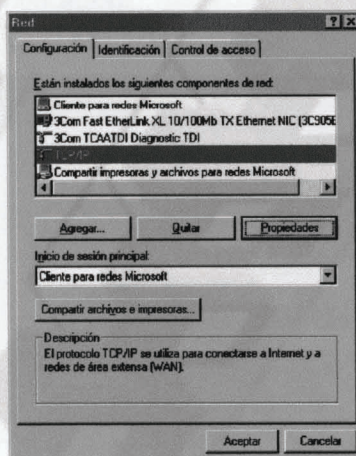
Un nuevo servicio llamado compartir impresoras y archivos para redes Microsoft ha aparecido. Si ahora hacemos doble click en Compartir archivos e impresoras podremos decidir si vamos a compartir archivos, impresoras, ambos o ninguno.



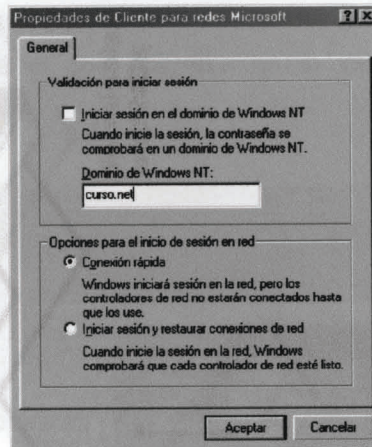
A partir de ahora podremos compartir impresoras y archivos utilizando el servicio instalado que a su vez utilizará al protocolo TCP/IP, el cual utilizará a la tarjeta de red instalada.

Cliente 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:



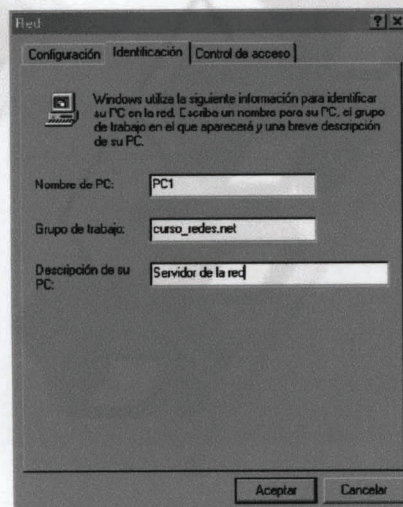
La primera opción que tenemos es iniciar una sesión en el dominio de Windows NT. Si en nuestra red existe un servidor NT y utilizamos recursos de este deberemos activar esa opción para que el servidor nos reconozca como usuarios y nos ofrezca sus servicios. Si la activamos nos pedirá un nombre de dominio, 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.

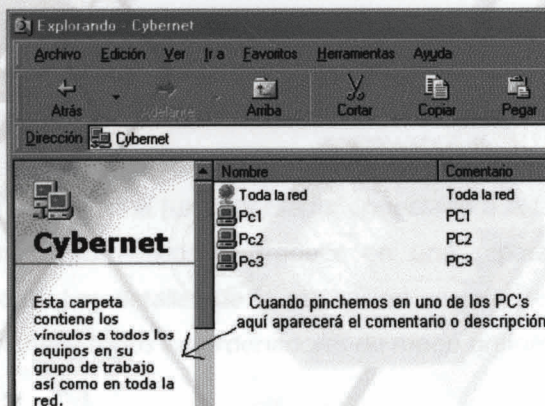
Con esto finaliza la configuración del Cliente para redes Microsoft.

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.

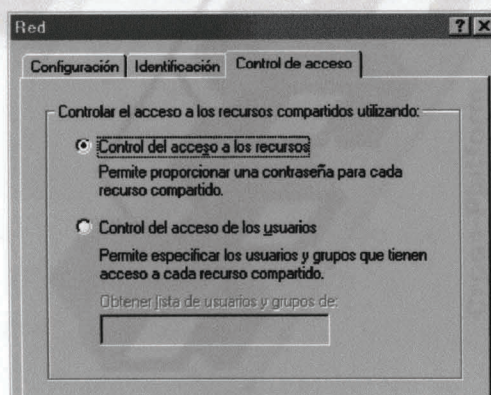


En esta ventana daremos un nombre a nuestro PC, podemos poner el que queramos. Este será el nombre con el que se verá a nuestro equipo en la red más adelante. También podemos introducir un comentario, este comentario será el que aparezca en la ventana de entorno de red cuando seleccionemos nuestro PC.



Un concepto importante que también aparece es el de grupo de trabajo. Recordemos que NT 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.

Resumen Cliente/servidor

En vez de construir sistemas informáticos como elementos monolíticos, existe el acuerdo general de construirlos como sistemas cliente/servidor. El cliente (un usuario de PC) solicita un servicio (como imprimir) que un servidor le proporciona (un procesador conectado a la LAN). Este enfoque común de la estructura de los sistemas informáticos se traduce en una separación de las funciones que anteriormente forman un todo. Los detalles de la realización van desde los planteamientos sencillos hasta la posibilidad real de manejar todos los ordenadores de modo uniforme.

Una red cliente/servidor permite a cualquier compañía compartir archivos y recursos comunes, tener acceso a la información en forma más eficiente; garantiza la seguridad y confiabilidad de los datos. Además, permite a todo el personal tener acceso a Internet, sin que esto represente un costo adicional.

En una red cliente/servidor, los "clientes" (ordenadores personales normales) se conectan a un "servidor" (un ordenador con más poder que "sirve" o facilita a los clientes datos, dispositivos y aplicaciones de *software*). Estas redes brindan grandes ventajas a los negocios. El servidor es típicamente una máquina de alto rendimiento que facilita compartir archivos grandes y permite a múltiples usuarios estar en la red, sin que esto ocasione demoras o problemas con el desempeño. También hace posible tener un alto grado de seguridad, para evitar que personal no autorizado use sus recursos. De igual forma, permite hacer respaldos de la información en forma centralizada. Además, brinda una plataforma para ejecutar aplicaciones compartidas, como soluciones de contabilidad o *software* de línea de negocios (como soluciones para inventarios o para manufactura).

Esta clase de red puede ser instalada en su empresa usando el *software* para servidor Microsoft NT Server y una variedad de *software* para cliente, ya sea, Windows NT Workstation, Windows 95 o Windows 98.

Caso Práctico I.

RED DE LA SECRETARÍA DE SALUD

ANTECEDENTES

En materia de redes y comunicaciones, la Secretaría contaba con muy pocas redes locales y enlaces electrónicos, a través de las cuales fluían los datos de las diferentes aplicaciones que operan a nivel nacional.

No se tenía la infraestructura de comunicaciones que se requiere para poder operar en línea, aplicaciones a nivel nacional que permitan mejorar el procesamiento de datos de los sistemas de información.

Algunas redes fueron instaladas con sistema de cableado no estructurado, lo cual complicaba la planeación de crecimiento de la red, proporcionando el servicio de red a unos cuantos departamentos de la unidad.

En cuanto a la red de voz, las unidades no contaban con equipos e instalaciones de comunicación de voz modernos, capaces de integrar la red global de comunicaciones de voz y datos, por lo que los gastos por mensajería llamados de larga distancia son muy elevados.

Con la ejecución de este proyecto, se cuenta con la infraestructura básica para la integración de la red global de comunicaciones de voz y datos de la Secretaría de Salud.

INTRODUCCIÓN

Descripción General del Proyecto a Nivel Nacional:

Se estudio con todo cuidado, todos y cada uno de los requerimientos y necesidades de la Secretaría de Salud para su programa de aplicación de cobertura en la Red Teleinformática y Sistematización.

La totalidad del proyecto contempla la instalación de una red global de comunicaciones a nivel nacional con servicios de voz y datos, que interconecta a todas y cada una de las unidades administrativas de la Secretaría de Salud, algunos de sus hospitales e instituto; fortaleciendo así la infraestructura de cómputo. Para lograr un fortalecimiento en la infraestructura de cómputo, se contemplo el diseño de redes locales, capacitación al personal y desarrollo e implementación de aplicaciones de cómputo que permiten obtener el máximo aprovechamiento de los recursos informáticos.

Esta primera fase fortalece la infraestructura de cómputo y de redes locales en las 32 entidades federativas y en algunas unidades administrativas a nivel central lo cual permitirá contar con una infraestructura mínima necesaria para automatizar las aplicaciones más importantes de tipo administrativo y sustantivo, así como las aplicaciones relacionadas con la automatización de algunas oficinas en internet.

Descripción General del Proyecto para el Estado de Michoacán:

Este proyecto de red se considera como la entrega e instalación de equipo de red, cableado y equipo de cómputo complementario para la implementación de una red local con cableado estructurado de voz y datos.

En cuanto al servidor, este se instaló trabajando sobre un software de red Windows NT con el Hardware y Software que se menciona en el presente documento. Así mismo, en esta red fueron instalados los equipos que se listan en el presente documento como equipo nuevo para la Secretaría de Salud además de dicho equipo se incluyeron en la red algunas computadoras propiedad de la Secretaría de Salud con procesadores que varían desde 150 Mhz hasta los 2.66 Ghz. Para esta instalación se utilizaron las tarjetas de red y se instaló en cada una de ellas el Software de cliente necesario para trabajar en la misma bajo plataformas que varían (D.O.S. Windows 95, 98, 2000 y Xp).

Es una red de tipo Ethernet de 10/100 MBPS cumplimiento con la IEEE 802.3 con una topología física y lógica de estrella.

Los servicios instalados en el cableado estructurado para Michoacán son los siguientes:

Nodos de Print Server	Servidores	Total de nodos de datos
3	2	85

Dado que la distancia máxima de un equipo Terminal con el servidor primario, no supera los 100 metros, se ha elegido utilizar el cableado UTP de categoría 5.

DESCRIPCIÓN TÉCNICA DEL CABLEADO DE DATOS Y DE VOZ DE LAS OFICINAS DE LA SECRETARÍA DE SALUD

El siguiente documento está estructurado para cumplir con las especificaciones de la SECRETARÍA DE SALUD para la realización del cableado de datos y de voz de sus oficinas. Dichas especificaciones contemplan los siguientes aspectos.

El material requerido para un sistema de cableado estructurado de voz y de datos categoría 5, que incluirá tubería, canaleta, cableado, centros de cableado, material de montaje, mano de obra y elementos necesarios para poner en marcha dicho sistema de cableado.

Así mismo, se utilizará tubo conduit pared gruesa en exteriores y pared delgada en el interior de los plafones, así como en aquellas áreas donde será necesario proteger los cableados contra daño mecánico o mal uso del personal. Se utilizara canaleta para cableado estructurado nivel 5 para datos y nivel 3 para voz especialmente sobre muros, es decir del plafón hacia abajo.

Estructura de cableado que se está proponiendo, permitirá un crecimiento continuo sin alterar los niveles de servicio que están ofreciendo.

Cuando la distancia del Site a los puntos remotos de servicio sea mayor a los 100 mts. Se tiene un problema de distancia, mismo que se debe resolver seleccionando la alternativa que más convenga, es decir, se podrá instalar un switch intermedio, utilizar fibra óptica, utilizar repetidor, etc.

Así mismo, para poner en marcha las instalaciones, se entregarán los planos de ingeniería de proyecto, procedimientos de instalación, cableado, administración y bitácora del proyecto.

A continuación se dan las especificaciones de la TUBERÍA que se instaló.

Los metros de tubería que se instalaron de pared gruesa en exteriores y pared delgada en interiores, galvanizados, con un diámetro que garantizó el 40% de espacio libre en el interior del tubo para instalaciones futuras. Dicha tubería quedo debidamente aterrizada eléctricamente.

La mayoría de los servicios se montaron sobre las paredes, sin embargo, cuando esto no es posible y se requiere un punto de servicio aislado de la pared, la ductería se hizo llegar sobre el techo del piso inferior, teniendo que perforar la loza para colocar el servicio donde se requirió.

Siempre fue necesario librar una columna se usó también tubo conduit pared gruesa galvanizada, preparando manualmente la curvatura que cada caso requiere. Se usaron codos prefabricados siempre y cuando no sea afectado el nivel de calidad requerido en este proyecto.

Para la sujeción de la ductería se utilizó solera de fierro y ángulo de acero, así como herramientas de alto impacto para la instalación de soportes, a su vez se instalaron clips tipo U de acero para montar la ductería sobre el soporte.

Todo el sistema de tubería quedó perfectamente acoplado, utilizando los componentes de acoplamiento que son necesarios, tales como coples, codos, terminadores, cajas de paso, etc.

Para exteriores se proporcionaron los elementos necesarios para garantizar el adecuado funcionamiento del sistema cableado. Así mismo, se proyectó la instalación de cajas de registro de paso a lo largo de las trayectorias largas, cada 20 mts. Y en cada cambio de dirección, con el objeto de facilitar la instalación y su funcionamiento. Así mismo, la tubería es pintada de color naranja para su identificación a línea de vista, cada 9 metros.

Para la instalación de la CANALETA se consideran los siguientes aspectos:

Se utilizó canaleta plástica de PVC.

Esta canaleta se instaló con los accesorios y acopladores que se requirieron, tales como esquineros, L's, T's y todos los accesorios que se requirieron, cumpliendo con los radios de curvatura necesarios que se requirieron, para la certificación de este mismo sistema de cableado estructurado.

Esta canaleta se utilizó para la canalización interna sobre muros, así mismo, se fijo mecánicamente a la pared, con puntos de fijación cada medio metro, independientemente de que cuente con adhesivo integrado; esta canaleta contó con un ancho mínimo de 1", aunque sólo alojó un cable.

Para la red de datos se utilizó cable UTP, categoría 5, de 4 pares de 100 ohms, 24 AWG que garantiza una transmisión de 10 a 100 Mbs. Así mismo, se utilizó para la red de voz cable UTP categoría 3 de 4 pares.

Todos los componentes de cableado cumplen con la normatividad NOM y UL.

Para la instalación de todas las líneas de cableado se identificaron cada 20 metros con una etiqueta sobre el conductor que especifica el segmento y el nodo al que pertenecen.

Las características de comunicación de este cableado están ajustadas a la norma IEEE 802. Aunado a esto, las trayectorias están diseñadas evitando cruces de fuentes de interferencia como EMI, RFI e impulsos generados por líneas de alta tensión, cableado de pararrayos, balastos, conductores eléctricos, radiación solar, computadoras, radares, motores, interruptores y otros objetos de similares características según los planos entregados por Secretaría de Salud.

Así mismo, todas las salidas están identificadas, tanto en racks como en las rosetas, con el número de servicio, segmento asignado y el número de servicio.

Para poder suministrar los servicios adecuadamente, los servicios de datos se conectaron al computador utilizando cables de línea (line cord) RJ45-RJ45 (AT&T D8AU-7) que están certificados por el fabricante que son de 2 metros de longitud, siguiendo la norma TIA/EIA 568, que están elaborados con cable de 4

pares categoría. De la misma manera, los cables de parcheo (patch cords) AT&T D8AU-5 y los cables de parcheo AT&T D8AU-3 y sus accesorios están certificados por el fabricante.

Todos los componentes del cableado cumplen con la normatividad NOM y UL y ser de la misma marca.

Para cableado de voz usaron cables riser categoría 3 desde el centro de cableado principal a los centros de cableado secundario, siempre que fue necesario colocar switch's intermedios para resolver distancias mayores de 90 mts.

Para toda la instalación se consideró prácticas de buen cableado como por ejemplo, el nivel de torcido de acuerdo a la categoría que se esta manejando, minimizando la parte desnuda en las terminales, así como no dejar suspendidos los cables, no apretar demasiado los paquetes de cables, además de usar los jumpers y patch coros correspondientes a la categoría que se está manejando.

Así mismo se especifica que el máximo retardo de propagación permitido es de 0.0512 ms en un circuito.

En lo que se refiere a los CENTROS DE CABLEADO se hacen las siguientes consideraciones.

En SITE principal (MDF) se utilizó rack cerrado con soportes delanteros rack mount, puerta de acrílico, barra de contactos, acceso frontal y posterior, ancho de 24", profundidad de 27", altura de 36".

Para los Estados de Tabasco, Tamaulipas, Veracruz, Tlaxcala, Yucatán, Zacatecas, así como para la Dirección General de Estadística e Informática, Contraloría General y el edificio de Informática la altura de los racks es de 72", en cambio para los estados restantes la altura es de 36".

En SDF's también se utilizaron rack's cerrados. Así mismo, entre los equipos activos de red y componentes de cableado estructurado se montaron sobre los racks mencionados.

Los remates del cableado se hicieron tanto en paneles de parcheo como en regletas. A su vez, estos sistemas de administración están diseñados considerado en las regletas de voz y datos un crecimiento del 50%.

Ahora, para realizar las bajadas del cable del sistema de ductería a los centros de cableado se uso tubería galvanizada pared gruesa con las curvaturas necesarias.

Los centros de cableado contienen:

Rack

Regletas con pares para necesidades actuales y crecimiento del 50%

Backboards con patas para la separación de los subsistemas

Connecting blocks

Sujetadores de cables

Anillos de distribución

Retenedores

Cables de parcheo nivel 5, certificados de fábrica

Cables de parcheo RJ45 del concentrador a la regleta ó panel de parcheo según sea el caso

Así mismo, el layout cumple con la norma ANSI/EIA/TIA-569.

En cuanto a las SALIDAS se consideraron los siguientes lineamientos.

Las salidas de voz y datos se colocaron a 35 cms. sobre el nivel del piso, a fin de evitar la acumulación de polvo y humedad en el jack.

Para todas las instalaciones, las rosetas para transmisión de datos son de un color y las rosetas para la transmisión de voz son de otro color, aunado a esto la roseta de voz está instalada a la izquierda, en tanto q la de datos se instalo a la derecha de la placa. La terminación de las salidas se hizo con jacks modulares RJ-45 categoría 5 para datos y categoría 3 para voz, contando con el estándar EIA/TIA T568A, con sus respectivos accesorios de montaje como el face plate y el dust cover. Así mismo las salidas están numeradas para su fácil identificación posterior; en el rack se numeraron las salidas, además de que cada roseta de datos se identifico con 2 dígitos adheridos en su parte posterior que corresponden a los del patch panel contando además del símbolo que corresponde al servicio que proporciona.

Las salidas se colocaron sobre el piso, se montaron sobre periscopios o patas de mula, con el objetivo de que dichas salidas queden debidamente protegidas.

El jack y la placa son de la misma marca (AT&T). Así mismo, las salidas son numeradas para su fácil identificación posterior. En el rack se numeraron las salidas de tal manera que si se cuenta con 2 o más paneles de parcheo, la numeración es consecutiva para todo el rack. Cada roseta de datos se identifico con dos dígitos adheridos en su parte posterior, que correspondieron a los del patch panel. Adicionalmente cada roseta tiene el símbolo que corresponde al servicio que proporciona, es decir, una computadora o un teléfono.

El CABLE UTP que se utilizó es AT&T 1061 con las siguientes características.

Numero de pares 4, No Plenum. Nivel 5
Conductor 24 AWG BC sólido
Aislamiento PE
Cubierta PVC retardante de flama
Impedancia a 20°C de 100 ohms +/-15% desde 1-100 Mhz
Resistencia DC A 20°C 28.6 ohms/305 m
Capacitancia mutua de 14 nanofaradios/305 m
Estándares EIA/TIA-568 y TSB-36
Atenuación máxima a 100 Mhz de 67 dB/305 m
NEXT a 100 Mhz de 32 dB

Los PATCH PANELES que se utilizaron tienen las siguientes características:

Patch panel sobre pared

Ensamblado en fábrica
Conductores de contacto del jack chapeado de 50 microns sobre níquel
Durabilidad de 750 inserciones
Presión del contacto 100 gramos por contacto

Patch panel sobre rack

Ensamblado en fábrica
Conductores de contacto jack chapeado en 50 microns sobre níquel
Durabilidad de 750 inserciones como mínimo
Panel de acero, calibre 22 a 26 AWG

Las SALIDAS que se utilizaron son AT&T M100BH para datos teniendo las siguientes características:

Corriente máxima de 1.5 amperes
Durabilidad de 750 inserciones
Presión del contacto de jack de 100 gramos

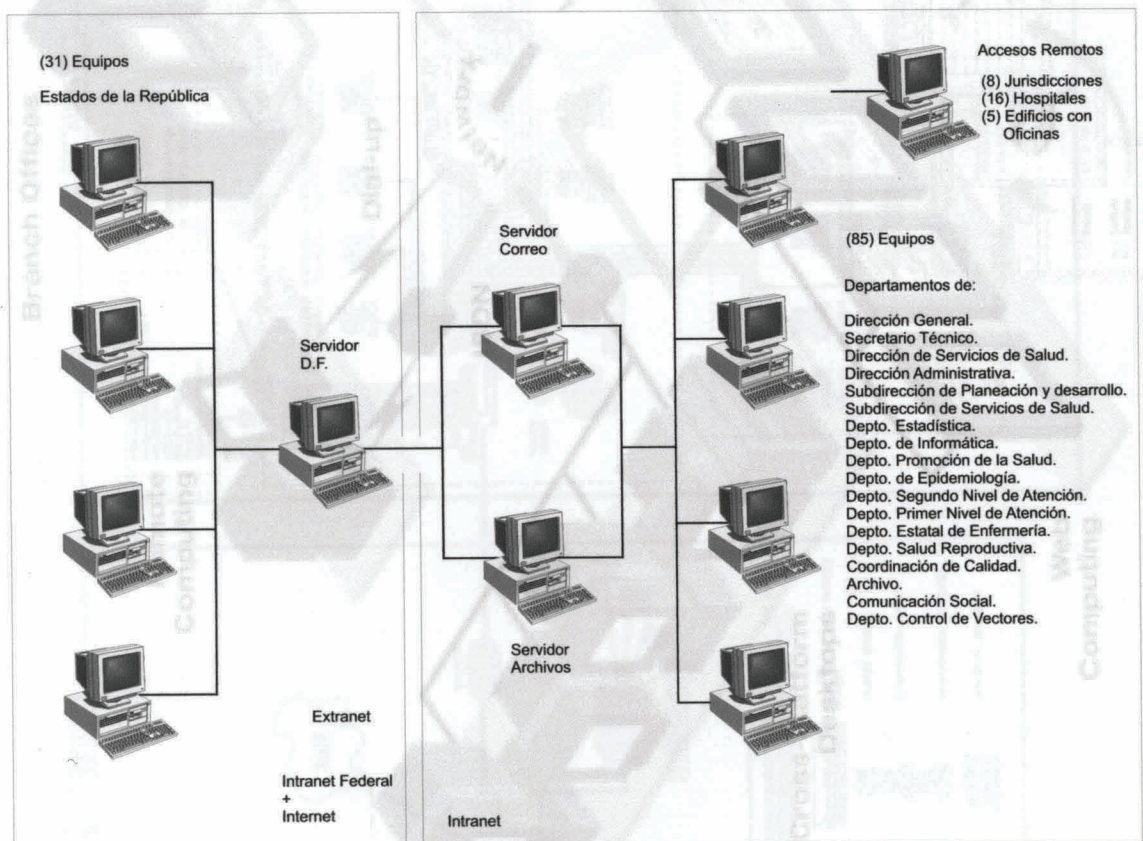
Los LINE CORDS que se utilizaron son AT&T D8AU-7 teniendo las siguientes características:

Categoría 5

- Cumplimiento de ANSI/TIA/EIA-568
- Conductores 24 AWG con aislamiento de termoplástico
- 4 pares torcidos individualmente
- Terminación en plug de 8 posiciones
- Cumplimiento de FCC
- Cumplimiento de UL 94-V2 (Flame Rating)
- Impedancia a 20°C de 100 ohms +/-15%
- Resistencia de 20°C de 28.6 ohms/305m
- Capacitancia max a 20° de 14 nF/305m
- Atenuación y Crosstalk que son similares a las del cable.

Las pruebas del sistema certificaron la transmisión a 100 mbps.

Esquema General de la conexión REDSSA al nivel nacional.



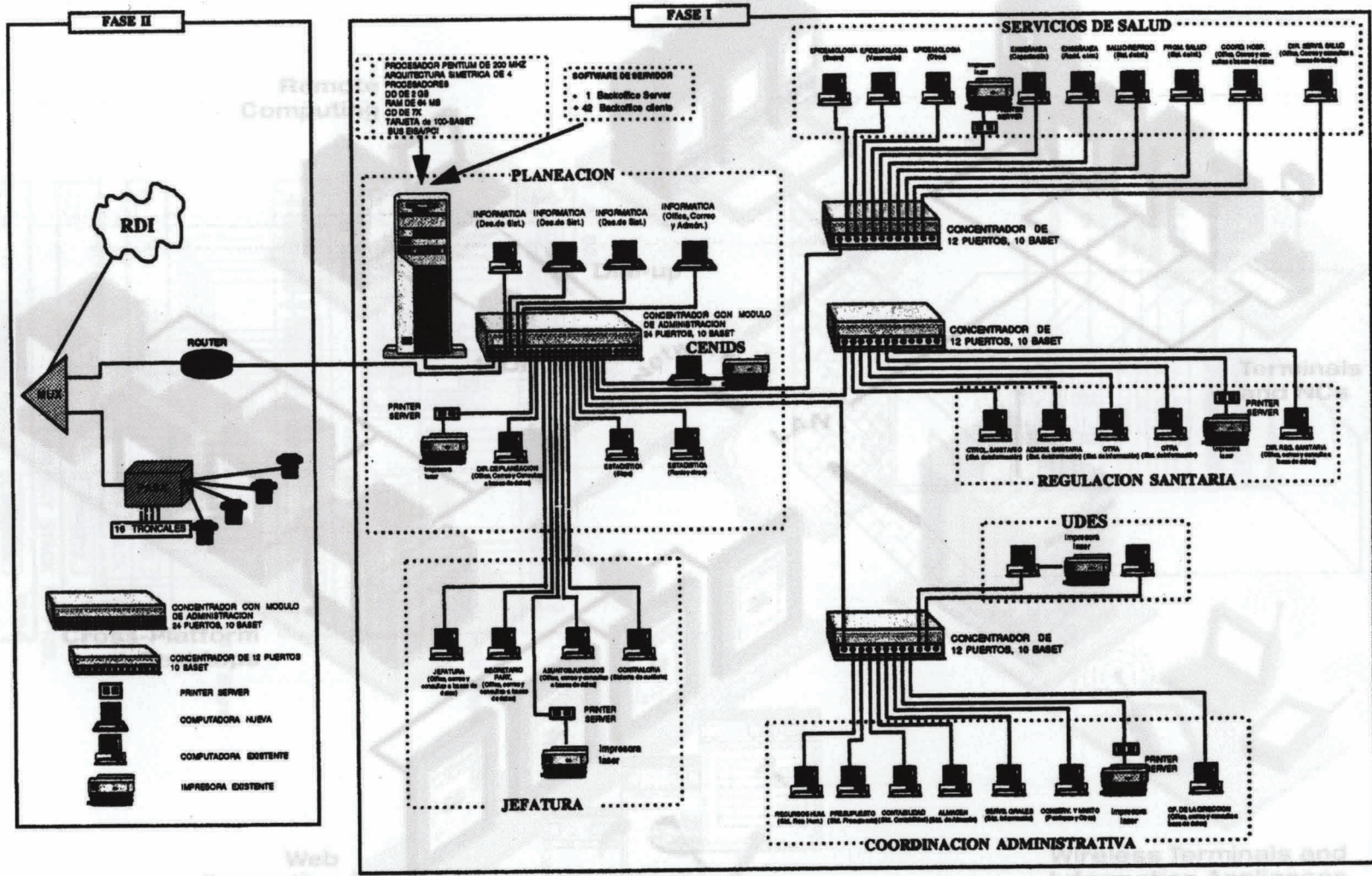


Figura 1. Redes locales de la SSM.

Figura 2. Rack de gabinete.

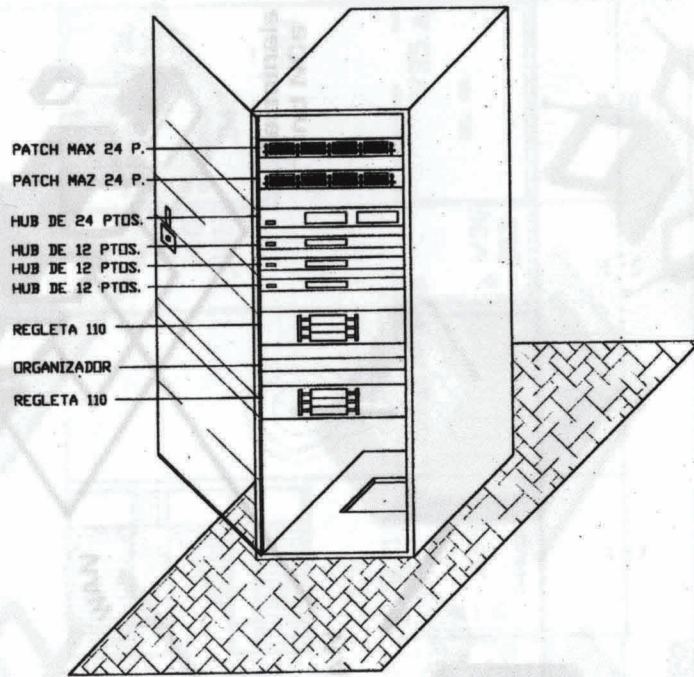


Figura 3. Panel de patcheo.

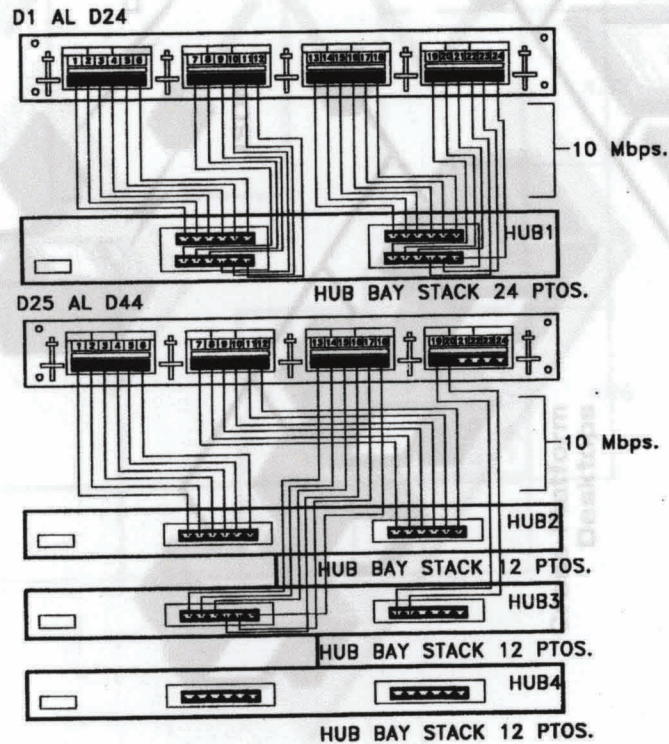
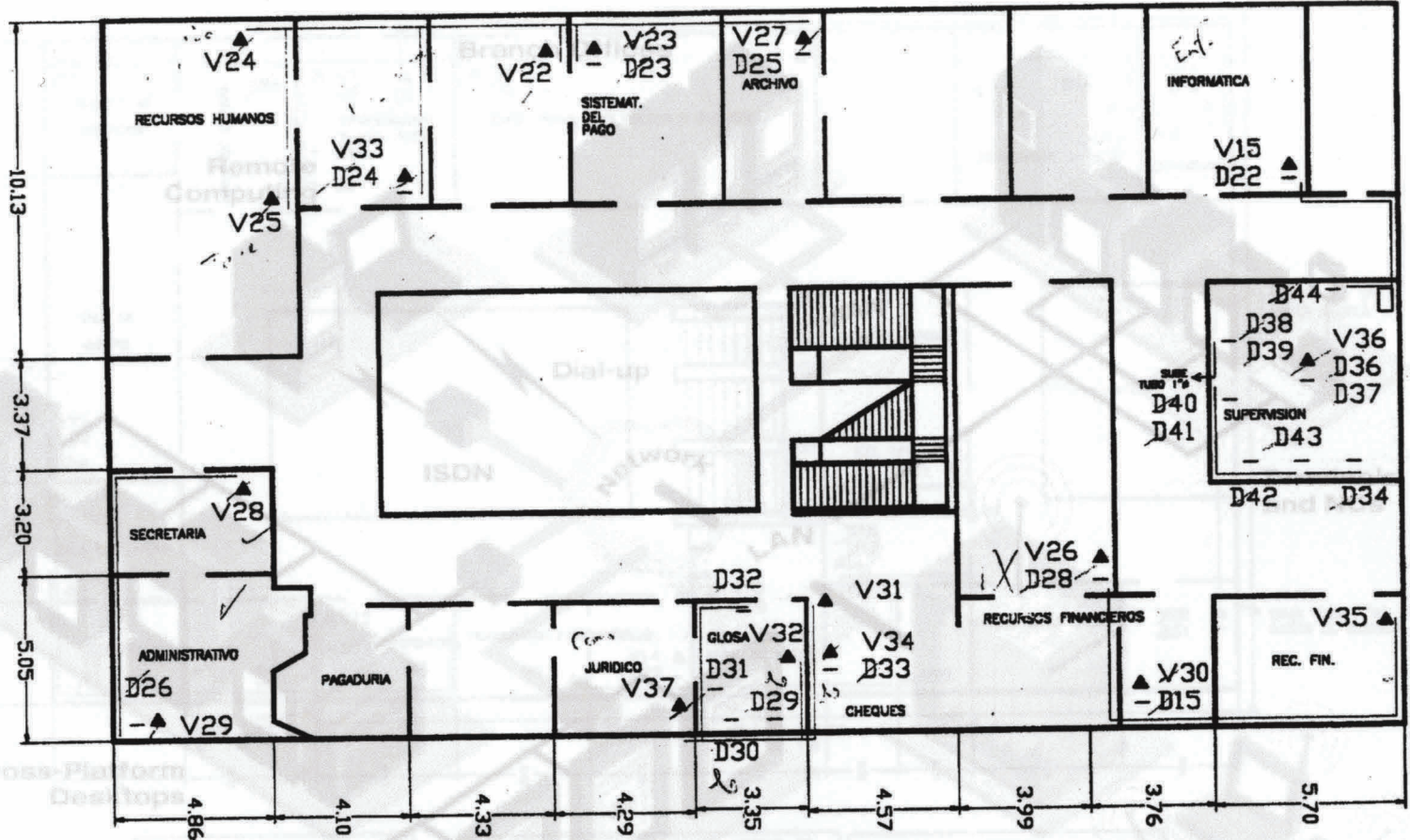


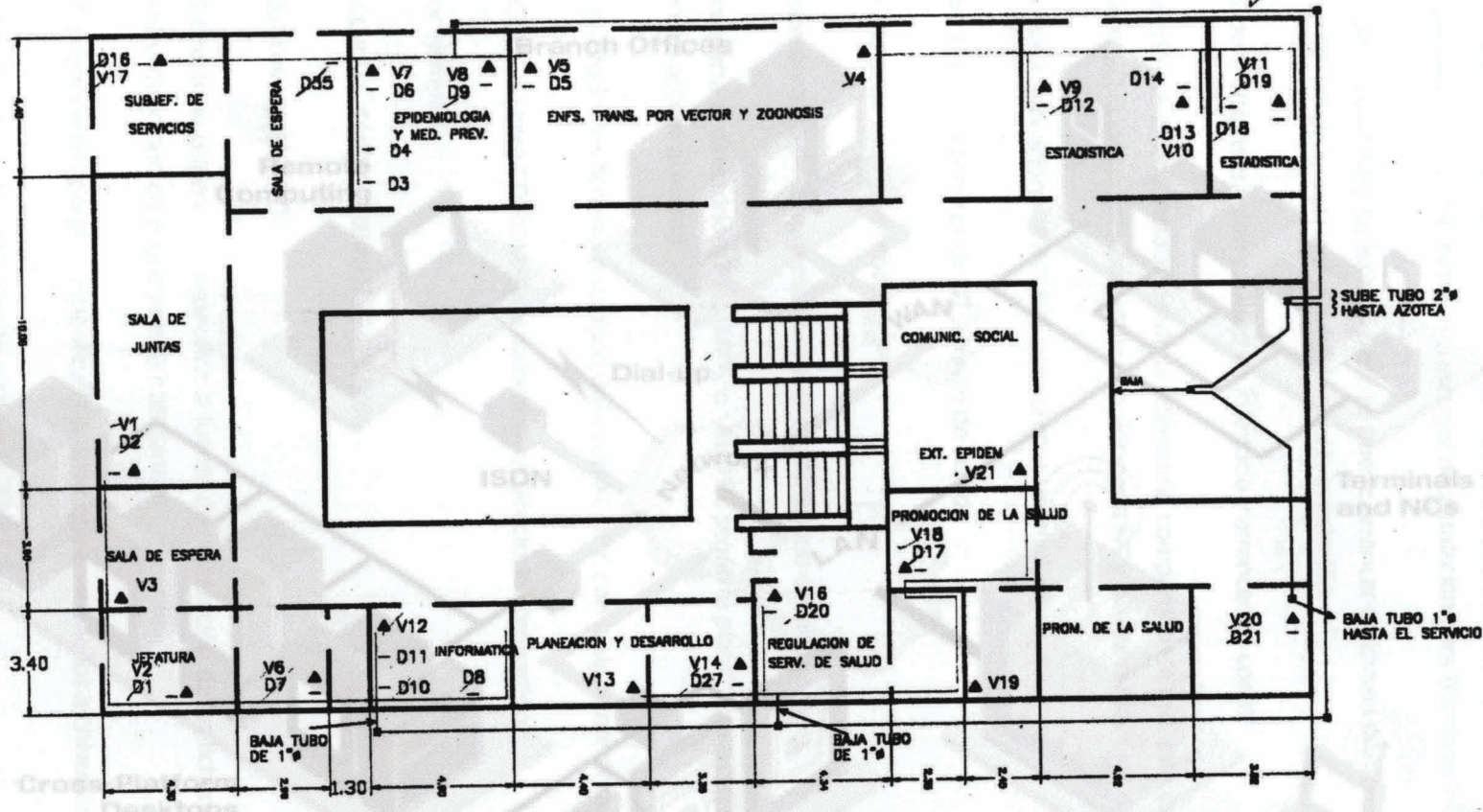
Figura 4. Diagrama físico (Planta baja).



SIMBOLOGIA	
—	CANALETA 35x17
□	RACK
▲	NODO DE VOZ
—	NODO DE DATOS

D.G.E.L. - Dirección de Planeación y Desarrollo Informático	
OPERA:	PLANTA BAJA
UBICACION:	MICHOACAN

TOTALES
SALIDAS DE DATOS = 20
SALIDAS DE PSERVER = 2
TOTAL = 22
SALIDAS DE VOZ = 17



SIMBOLOGIA	
—	Tubo 1"ø
- - -	Tubo 2"ø
—	Canaleta 35x17
⊠	Registro 12x12
▲	Nodo de Voz
■	Nodo de Datos

DIRECCION DE SALUD	
D.G.E.L. - Dirección de Planeación y Desarrollo Informáticos	
UBICACION	PLANTA
PLANO PARA LA RED	PLANTA ALTA
ESTADO	FECHA
MICHIGAN	JUNIO-87
PROYECTO RED 80A	

TOTALES
SALIDAS DE DATOS = 22
SALIDAS DE PSERVER = 3
TOTAL = 22
GLOBAL DE DATOS = 44
SALIDAS DE VOZ = 20
GLOBAL DE VOZ = 37

Figura 5. Diagrama fisico (Planta alta).

La instalación de Windows NT.

Windows NT se adquiere en CD-ROM. Además vienen con él tres discos de arranque. Dependiendo de su hardware, tiene dos métodos a escoger de instalación para Windows NT Server o Workstation:

Desde el CD-ROM, si su BIOS lo permite puede arrancar el sistema desde el CD-ROM (ver Boot Sequence en el SETUP de su sistema) y comenzar así la instalación.

Desde la disquetera, con el Disco #1 insertado y arrancando con él.

También se puede instalar desde un directorio compartido de red, esta es una solución al problema de que el CD-ROM no sea compatible con Windows NT y no queramos usar disquetes.

Se usa la aplicación WINNT.EXE para preparar el equipo.

Para copiar los ficheros de NT a través de la red.

La red debe estar operativa.

Tiene permiso de lectura-escritura sobre el directorio destino.

Comparta el directorio \I386, \MIPS, o \ALPHA, según la plataforma a instalar que está en el CD-ROM, así tendrá acceso al mismo.

Copie todos los ficheros a su disco duro con XCOPY, con la siguiente sintaxis:

```
XCOPY /s <letra CD-ROM>:\<plataforma> \<Directorio compartido>
```

Por ejemplo:

```
XCOPY /s F:\I386 \WINNT35.SRC\X86
```

Opciones de WINNT:

/S directorio origen especifica la fuente de localización de los ficheros de Windows NT, por defecto será el directorio en el que se está trabajando.

/T directorio temporal especifica la unidad que contiene los archivos temporales de instalación.

/I información localización del archivo DOSNET.INF

/X no se crean los discos de instalación

/F no se verifica la copia de los discos

/O sólo se crean los discos de instalación

/OX esta opción crea los discos de instalación para instalar desde CD-ROM o disquetes.

La instalación es muy parecida a la de Windows 95 y los pasos son los siguientes:

Ejecute el programa SETUP.EXE desde el CD-ROM.

Elija entre instalación rápida o personalizada.

Especificar si se actualiza de una versión existente de Windows NT o se instala de nuevo.

Proporciones información sobre su nombre de usuario, nombre de ordenador. Especificar qué lugar ocupará este equipo en la seguridad de la red.

Elija el lenguaje que desea usar.

Si elige el SETUP personalizado, decida sobre las opciones a instalar. Si por el contrario, ha decidido realizar la instalación rápida, se instalarán todas las opciones.

Instale su tarjeta de red y seleccione el protocolo de red por defecto.

Instale su impresora local, si la tiene.

Instale la contraseña o password para el administrador de la red.

Ponga la hora local, especifique el tipo de adaptador de vídeo y haga un disco de reparación de emergencia.

NOMBRE DE SERVIDORES Y DOMINIOS

Para el nombre del servidor se uso la abreviatura del nombre del Estado o nombre de la unidad administrativa, seguida de un guión "-" y una D.

Red del Estado de Michoacán = MICH-D

Para el nombre del dominio se uso la abreviatura del nombre del Estado o nombre de la unidad administrativa, seguida de un guión "-" y una D.

Red del Estado de Michoacán = MICH-D

DIRECCIONAMIENTO IP

- Para el funcionamiento de la red WAN de voz y datos, se requiere que todos los clientes de NT, manejen el protocolo TCP/IP para poder rutear hacia otras redes.
 - La dirección de host asignada al servidor es: 130.16.1.1
 - La dirección para el ruteador es: 130.16.1.2
 - Para numerar las estaciones de trabajo, se habilitaron los servicios de DHCP con los siguientes parámetros: 130.16.1.3 – 130.16.1.255
- 1) Para definir el rango de direcciones disponible por DHCP se incluyeron las direcciones del servidor y la del ruteador.
 - 2) La máscara es de 8 bits, es decir 255.255.255.0

SEGURIDAD

- Creación de los discos Emergency Disk Repair y el disco con la información de las particiones del disco duro del servidor
- Windows NT se encuentra instalado en una partición FAT, por que en caso de falla se pueden restaurar los archivos de NT sin problema
- Respalidar periódicamente en cinta, la información contenida en el servidor
- Es importante educar a los usuarios en la asignación y uso de passwords para garantizar la seguridad de la información de los mismos, para ello se pueden crear passwords con longitud de hasta 14 caracteres alfanuméricos.
- Apagar el equipo utilizando el comando shutdown.
- Mantener la bitácora de red actualizada.

Caso Práctico II.

Red Local de la Unidad Estatal de Protección Social en Salud.

Introducción.

Esta unidad de la Secretaría de Salud es de reciente creación, sin grandes requisitos de comunicaciones tanto para el nivel estatal como para el nivel federal, por lo tanto se instaló una pequeña red LAN, en el edificio donde opera esta unidad.

La red local es para compartir servicios y periféricos, como son las impresoras, scanner, el Internet y archivos de trabajo, las comunicaciones con otras oficinas y/o dependencias se realiza a través del correo electrónico por Internet. Para comunicación intra dependencia se utiliza un mensajero electrónico para área local.

Las aplicaciones que generalmente utilizan los usuarios son las del Office, Sistemas Internos (Stand Alone), algunas aplicaciones de edición de imágenes y diseño vectorial, además del uso del Internet para las comunicaciones o consulta de información.

Los equipos con que cuenta esta unidad varían en su velocidad de procesamiento, desde 1.8 Ghz hasta los 3 Ghz, todos están conectados por medio de ethernet, distribuidos de la siguiente manera:

Ubicación	Cantidad de Equipos
Dirección	1
Subdirección de Gestión	1
Subdirección de Promoción y Afiliación	1
Depto. Costos y Presupuestos	2
Depto. Promoción y Afiliación	2
Depto. Administración del Padrón	3
Sala de Juntas	3
Informática	1

La unidad cuenta también con 5 impresoras disponibles, de las cuales 3 están conectadas al equipo que funge como servidor y la restante cuenta con la posibilidad de conectarse directamente en red a través del switch. Por comodidad el equipo de la Dirección cuenta con su propia impresora

La topología implementada en la red de la unidad es la de estrella, tanto física como lógicamente.

Los materiales utilizados para la interconexión de los equipos anteriormente citados fueron los siguientes:

- Canaleta PVC.
- Cable UTP Categoría 5
- Conectores RJ45
- Tarjetas de Red de 100 Mbps.
- Switch de 16 puertos.

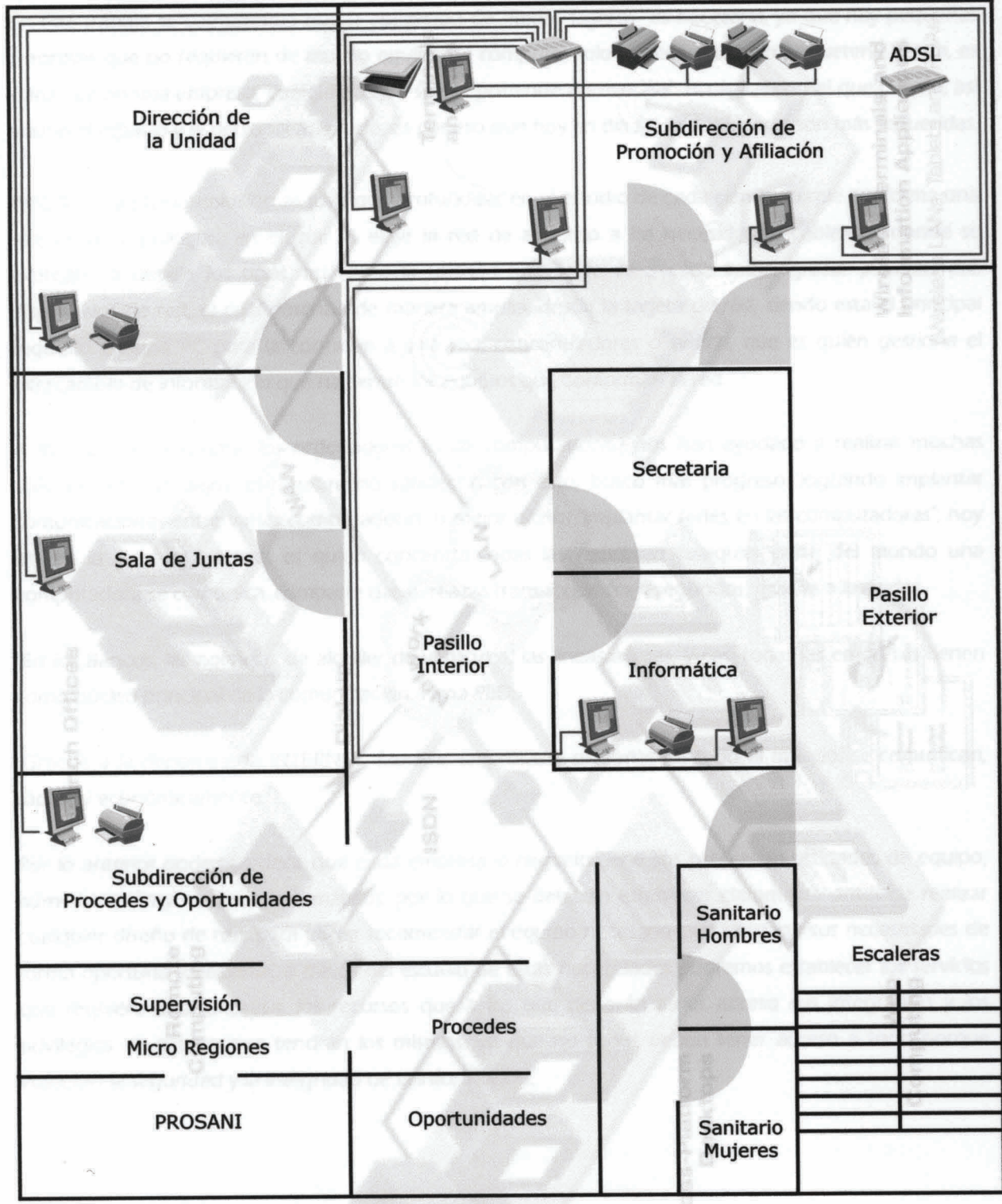
El servicio de Internet se proporciona a través de un equipo que tiene instalado y configurado dicho servicio con un cable modem Toshiba PCX1100U, con una conexión de 512 Kbps, a su vez comparte el servicio a los demás host de la red local mediante el uso de Windows Xp.

La designación de direcciones IP para cada host se hizo de manera secuencial tomando como base una red privada clase C (192.168.0.X).

Se tiene instalado en el equipo que comparte el servicio de Internet, un firewall para la protección de los datos y equipos dado que de otro modo estarían expuestos al exterior. Así mismo cada equipo tiene instalado un antivirus y actualiza constantemente su sistema operativo.

Cabe mencionar que existe la posibilidad de cubrir satisfactoriamente el crecimiento en cuanto equipos conectados sin ningún cambio en el diseño inicial, hasta los que físicamente podrían tener todos los integrantes de la unidad teniendo un equipo cada uno de ellos.

Diagrama Físico.



CONCLUSIONES.

En este trabajo se comprendió que la aplicación de "Redes Ligeras" es necesaria, ya que hay pequeñas empresas que no requieren de mucho equipo de cómputo, solo lo necesario, con paquetería básica, es claro que en una empresa, cualquiera que sea se pretende aprovechar el capital con el que cuenta, así mismo el espacio y el personal asignado, es por eso que hoy en día las Redes Ligeras son más requeridas.

Para llegar a esta conclusión se tuvo que profundizar en el estudio de cada elemento que conforma una red; desde topologías, en el que se elige la red de acuerdo a las necesidades; cableado, donde se explican a detalle los tipos, así como la utilidad que se le da a cada cable, grosor, rapidez, etc. dispositivos de red, el cual describe de manera amplia, desde la tarjeta de red, siendo esta el principal requisito en una PC para la conexión a una red, concentradores o switch, que es quién gestiona el intercambio de información que hay entre los equipos que conforman la red.

A lo largo de la historia los ordenadores (o las computadoras) nos han ayudado a realizar muchas aplicaciones y trabajos, el hombre no satisfecho con esto, buscó mas progreso, logrando implantar comunicaciones entre varias computadoras, o mejor dicho: "implantar redes en las computadoras"; hoy en día la llamada Internet es quién concentra todas las redes, en cualquier parte del mundo una computadora se comunica, comparte datos, realiza transacciones en segundos, gracias a las redes.

En los Bancos, las agencias de alquiler de vehículos, las líneas aéreas, y casi todas las empresas tienen como núcleo principal de la comunicación a una RED.

Gracias a la denominada INTERNET, familias, empresas y personas de todo el mundo, se comunican, rápida y económicamente.

Por lo anterior podemos decir que cada empresa o negocio tiene sus propias necesidades de equipo, administración y recursos informáticos, por lo que se deberán establecer claramente antes de realizar cualquier diseño de red, para poder recomendar el equipo necesario que satisfaga sus necesidades de forma oportuna y eficiente, a través del estudio de estas necesidades podremos establecer los servicios que requiere una empresa, los recursos que a los que deberán tener acceso sus integrantes y los privilegios de acceso que tendrán los mismos, ya que no todos deben tener acceso a todo porque vulneran la seguridad y la integridad de la información.

RECOMENDACIONES.

Como recomendación para mejorar la eficiencia respecto a la red que actualmente se encuentra instalada en la Secretaría d Salud:

- Modificar el Site, ya que las condiciones en las que se encuentra no son las adecuadas.
- Asignar una pequeña área del edificio específica para el Site de la Secretaría de Salud que no sea visible al público ni accesible a personas ajenas.
- Crear el piso o el techo falso con el que actualmente no se cuenta, esto ayudaría con una mejor organización de los cables y daría un mejor aspecto al Site.
- Cambiar los switch por modelos que sean administrables, esto significaría mayor rapidez en el tráfico de información, más seguridad y un mejor rendimiento en las operaciones creadas en la red, ya que nos permitiría un mayor control sobre las redes y las ip's asignadas, ya que es una red utilizada a nivel nacional.
- Implementar un clima para mantener el Site a la temperatura requerida que es de 18°C, esto mejoraría el rendimiento en todos los periféricos por los cuales circula la información.
- Restringir el acceso del personal, limitado a 2 o 3 personas previamente capacitadas para dar el mantenimiento y manejo del Site, así como de los servidores, asignar claves para el acceso y privilegios para modificar lo que se requiera.
- Implementar medidas de seguridad necesarias, como extintores, tomas de agua, reguladores de electricidad, salida de emergencia, esto ayuda para prevenir grandes daños en caso de accidentes.
- Crear planes de contingencia en caso de desastres.
- Crear grupos de usuarios con privilegios establecidos de manera clara y acorde a las necesidades de acceso de cada usuario que pertenezca al grupo.
- Tener un plan de mantenimiento preventivo de al menos dos veces al año para mantener en óptimas condiciones el equipo que hace posible el funcionamiento de la red.

BIBLIOGRAFIA

Textos Consultados:

"Redes de comunicación", Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation. Reservados todos los derechos.

Redes locales, José Luis Raya, Cristina Raya, 2ª edición, edit. Alfa Omega Ra-Ma, Año 2003.

Guía Rápida Para el Administrador de Red, Emilio Bocau, Edit. Trillas, año 2000.

Sistemas de Información, Timbal P. Marshal, edit. Thomson, Año 2001.

El Registro de Windows 2000, Katy Ivens, edit. Norma Interamericana, Año 2000.

Desarrollo y Gestión de Proyectos Informáticos, Donoban Galiley, edit. Mc Graw Hill, Año 2000.

Redes – Iniciación y Referencia, Jorge Sánchez , Jorge López, edit. Mc Graw Hill Interamericana, año 2000.

REDES DE COMPUTADORAS, Andrew Tanenbaum, Editorial McGraw Hill. México 1997.

REDES DE COMPUTADORES, PROTOCOLOS, NORMAS E INTERPRETE, Wyless Black, Alfa Omega Grupo Editor.

En Internet:

<http://www.ts.es/doc/area/produccion/ral/BANDA.HTM>

<http://www.cybercursos.net/cursos-online/lan/>

<http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html>

<http://www.ts.es/doc/area/produccion/ral/CABLE.HTM>

<http://www.monografias.com>

<http://www.geocities.com/Eureka/Plaza/2131/primeras.html>

<http://www.geocities.com/nicaraocalli/>

<http://www.internautas.org/NOTICIAS/DIC98/ADSL.htm>

<http://www.htmlweb.net/redes/osi/osi.html>

http://www.brain.com.mx/Soluciones/brain_y_las_redes.htm#red_punto_a_punto

Glosario de términos.

10 BASE 2	Implementación de Ethernet de 10 Mbps en cable coaxial delgado. Su máximo segmento es de 200 metros.
10 BASE 5	Implementación de Ethernet de 10 Mbps en cable coaxial grueso. Su máximo segmento es de 500 metros.
10 BASE F	Especificación para red Ethernet de 10 Mbps en fibra óptica.
10 BASE T	Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.
100 BASE FX	Especificación para correr Ethernet 100 Mbps sobre fibra óptica.
100 BASE T	Estándar de transmisión sobre MIT de velocidad 100 Mbps.
100 BASE T4	Especificación para correr Ethernet 100 Mbps sobre cable 3,4 y 5 MIT de 4 pares.
100 BASE TX Address	Esquema que ofrece 100 Mbps sobre cable categoría 5 MIT. En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.
Administrador	Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman superusuario.
Algoritmo	Serie de pasos para realizar una tarea específica.
Ancho de banda	Relación de velocidad para la transmisión de datos medidos en Kbps (kilo baudios por segundo) y que representa la capacidad del canal de comunicación para transportar datos.
ANSI	Organización encargada de la documentación de los estándares en Estados Unidos.
APPC	Protocolo de comunicación de dos equipos donde no existe director.
Application Server	Computadora destinada a brindar los servicios de una aplicación específica a los usuarios de una red.
ARCNet	Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.
ARP	Proceso en donde se asigna al número de la tarjeta una dirección formato TCP/IP.
ARPA	Agencia militar de Estados Unidos encargada de proyectos tecnológicos como las redes computacionales militares.
ARPANET	Proyecto del Departamento de Defensa de los Estados Unidos que utiliza protocolos tipo X.25 donde la cantidad de información (paquetes) no es fija. La dividieron en dos: Milnet para uso militar e Internet para uso público.
ASCII	Código utilizado para representar los caracteres de escritura en formato binario (7 bits para 128 caracteres o el modo extendido de 8 bits para 256 caracteres).
Asíncrona	Forma de transmisión de datos donde no se necesita señal adicional de reloj. La señal contiene la información de cuándo cambia cada dato.
ATM	Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.
AUI	Conexión utilizada para poder cambiar de tipo de cables en topologías Ethernet.
Average seek	Intervalo promedio de tiempo desde que el sistema solicita datos hasta que dispositivo los tiene

Wireless Terminals and
Information Appliances
(Wireless LANs, Tablets, etc.) P.246

Remote
Computing

Web
Computing

Backbone network	disponibles. Red de Infraestructura. Red que actúa como conductor primario del tráfico de datos de la red. Comúnmente recibe y manda información a otras redes.
Backup server	Servidor dedicado a realizar las copias de seguridad y restaurar los datos borrados por error de toda la información de la red.
Baud rate	Unidad de velocidad igual a un bit por segundo.
BIOS	Porción de firmware de una computadora que maneja el flujo de señales entre el sistema principal y los dispositivos periféricos. Controla puertos, memoria, teclado y dispositivos primarios.
BIT	Dígito binario, unidad mínima de información de los dos estados 0/1. Abreviación de Binary Digit que puede ser 0 o 1. Es la unidad básica de almacenamiento y proceso de una computadora. 8 bits = 1 byte.
BOOT	Proceso inicial por el que se cargan los programas para el total funcionamiento de la computadora.
BPS	Bits por segundo. Velocidad de transmisión serial.
Bridge	Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.
Broadcast	Transmisión abierta. Mensajes que se mandan sin destino específico.
Buffer	Espacio físico de memoria destinado a guardar datos temporalmente.
BUS	Circuito de interconexión eléctrica para transmitir información.
Byte	Conjunto de 8 bits. Representa un carácter en lenguaje binario.
CABLE NIVEL 3	Cable tipo MIT 2 pares que soporta 10 MHZ.
CABLE NIVEL 4	Cable tipo MIT que soporta 20 MHZ.
CABLE NIVEL 5	Cable tipo MIT 4 pares que soporta 100 MHZ.
Caché	Memoria más cercana al CPU, es utilizada como buffer entre el CPU principal y el resto de la computadora. Normalmente es la memoria de más rápida, fina y cara por ser la que más se ocupa.
Carrier o portadora	Señal eléctrica que permite la modulación de otra señal que contiene la información. Se utiliza para la transmisión remota vía la infraestructura de comunicaciones.
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía. Encargado de los estándares internacionales de comunicación.
CD-ROM	Memoria de lectura grabada en tecnología láser de CD.
CHIP SET	Referente al grupo de circuitos integrados que se utilizan para una función.
Cliente	número de pistas en los diferentes discos físicos. Producto o presentación de front end (directamente con el usuario) que interactúa con otros servidores o productos de back end (sin presentación directa con el usuario). El cliente realiza solicitudes y presenta los resultados. No realiza los procesos ni los cálculos, eso se los deja a los programas de back end que son más poderosos pero no tienen la capacidad de comunicarse directamente con el usuario.
CMOS RAM	Memoria no volátil de lectura. Escritura que almacena la configuración del sistema.
Colisión	Definido como un exceso en portadora eléctrica. Sucede

Wireless Terminals and
Information Appliances

Wireless LANs, Tablets and PDAs

Branches

Remote
Computing

Web
Computing



	en Ethernet cuando dos o más estaciones hablan al mismo tiempo y las señales de datos se pierden.
Communication Server	Computadora destinada a dar los servicios de comunicaciones de la red.
Concentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.
Conectividad	Estado que permite la transferencia de datos entre dos computadoras.
CPU	Unidad de Proceso Central. Director y principal realizador de procesos de la computadora. Circuito microprocesador que realiza los procesos de datos básicos y controla el funcionamiento general de la computadora.
CSMA/CD	Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.
Data Address	Localización física dentro del dispositivo de almacenamiento.
DDP	Tipo de conexión a Internet creado por Datasys de América. Se lleva a cabo por medio de una línea telefónica que comunica a la computadora del cliente con el ruteador que da acceso a Internet. Mantiene velocidades de 56.4 Kbps y tiene la capacidad de alimentar una red de hasta 10 computadoras. Para su instalación, el DDP necesita: dos modems idénticos de 28.8 Kbps conectados a la computadora cliente y al ruteador del proveedor; instalación de Windows NT en la computadora cliente, y de una configuración especial para el ruteador del proveedor. Este producto elimina el ruteador del lado del cliente.
Dial Up	Circuito de comunicación que se establece vía telefónica.
Dirección Destino	En el lenguaje de redes es la computadora que envía los datos de una transmisión.
Dirección Fuente	En el lenguaje de redes es la computadora que recibirá los datos en una transmisión.
DLC	Protocolo para el manejo de datos a través de líneas de comunicación.
DMA	Procedimiento de bajo nivel que permite que un dispositivo secundario de puertos (externo) tenga acceso a los recursos de memoria sin que el microprocesador tenga que atender el proceso. ISA Compatible/8 ciclos de reloj/960 ns. EISA tipo A/6 ciclos de reloj/640 ns. EISA tipo B/4 ciclos de reloj/480 ns. EISA tipo C/1 ciclos de reloj/120 ns. EISA tipo F/3 ciclos de reloj/360 ns.
Dominio	Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.
DOS	Sistema operativo más usado en PC's.
Drive	Dispositivo que permite el alojamiento de un tercer elemento para completar un dispositivo (por ejemplo: un drive de cinta es el hardware que permite leer y escribir en una cinta).
Driver	Manejador. Es el programa que contiene el algoritmo de

	manejo de un tercer elemento para poder manejarlo como otro dispositivo (ejemplo: el programa que nos permite manejar una tarjeta de red como otro dispositivo es el driver).
DS0	Enlace de comunicación dedicado sencillo. Canal digital de ancho de banda igual a 64 Kbps.
DS1	Canal de comunicación digital de señal tipo 1; puede ser E1 de 1.44Mbps en Estados Unidos o T1 de 2.108 Mbps en el estándar europeo.
DS3	Canal de comunicación digital de señal tipo 3; puede ser de 44.736 Mbps.
DS4	Canal de comunicación digital de señal tipo 4, de 274.176 Mbps en estándar de Bell.
DTE	En redes, son los equipos en donde los datos tienen origen y destino.
E0	Término utilizado para referirse a los canales de ISDN de 64 Kbps en estándar americano.
E1	Estándar europeo de transmisión de datos 2.048 Mbps.
E3	Canal de comunicación digital de 34 Mbps. El más veloz del mercado.
EEC	Método que consiste en grabar información adicional para poder corregir algún dato que se borre.
ECMA	Fija los parámetros de fabricación para los equipos de cómputo en Europa.
EISA	Estándar de intercomunicación entre CPU/motherboards y tarjetas secundarias, dispositivos de I/O, bus AT mejorado de 32 bits compatible a ISA y con las ventajas de MCA.
E-mail	Correo que se establece vía electrónica mediante Internet. Cada persona tiene una dirección asignada en su computadora de tal manera que puede enviar y recibir mensajes.
Encriptamiento	Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.
EOT	Señal que se manda para indicar dónde termina una transmisión.
Escalabilidad	Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y tarjetas periféricas.
Estación Ethernet	Computadora que puede realizar procesos. Estándar de red más popular e implementado. Utiliza CSMA/CD con una velocidad de 10 Mbps.
Fast Ethernet	Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.
FAT	Archivo que utiliza DOS para saber la ubicación física de los archivos en un medio de almacenamiento.
FDDI	Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token Ring/Token Passing.
File Server	Computadora dedicada a proveer y almacenar los archivos.
Firewall	Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.
Firmware	Conjunto de programas de sólo lectura que contienen el algoritmo para una función específica. Algoritmo o pequeño programa de bajo nivel grabado en un EEPROM para

Wireless Terminals and Information Appliances
Wireless LANs, Tablets and PDA's

Branch Offices

Remote Computing

Web Computing

Frame Relay	uso del procesador. También se llama Microcode. Paquetes retrasados. Protocolo de comunicación asíncrono con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño fijo.
FTP	Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.
Full Duplex	Característica de un canal de comunicación en el que dos terminales pueden mandar y recibir información simultáneamente.
Gateway	Dispositivo que permite conecta dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.
Gigabyte GUI	GB, 1 073'741 824 bytes, formalmente es 1 K de MB. Medio de desplegar las salidas para presentar al usuario un formato gráfico.
Half duplex	Característica de un canal de comunicación en el que dos terminales mandan y reciben información turnándose, una a la vez.
Hamming Code	Código de detección de errores de comunicación que consiste en enviar bits adicionales con la información acerca de los datos transmitidos para poder compararla en su destino.
Hardware	Referente a dispositivos reales, físicos. Todos los componentes electrónicos, magnéticos y mecánicos de las computadoras.
HDLC	Protocolo para redes X.25.
Hexadecimal	Sistema numérico con base en 16, comúnmente utilizado por su estructura fácil de transformarse al binario.
Hipertexto	También llamado Texto Virtual. Se refiere a la capacidad de recibir información en múltiples dimensiones. Una línea de texto puede llevar a otro texto, una imagen o una melodía.
Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.
Hub	Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal (retiming), y retransmisión de la misma (repeating).
ICMP	Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.
IEEE	Agrupación de ingenieros que, entre otras funciones, documenta todos los desarrollos tecnológicos.
IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).
IEEE-802.4	Define cuadros Token Bus tipo ARCNET.
IEEE-802.5	Define hardware para Token Ring.
IEEE-802.6	Especificación para redes tipo MAN (de área metropolitana).
IEEE-802.7	Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
IEEE-802.8	Especificación para redes de fibra óptica tipo Token

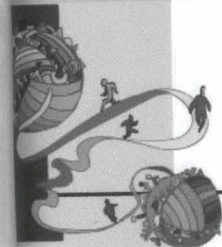
Wireless Terminals and Information Appliances
Wireless Labs, Tablets and PDA's

Branch Office

Remote Computing

Web Computing

Cross-Platform Desktop



	Passing/FDDI.
IEEE-802.9	Especificaciones de redes digitales que incluyen video.
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.
IEEE-802.12	Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.
IEEE-802.14	Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.
Interface	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Internetworking	Término usado para referirse a la interacción entre varias redes.
Interoperabilidad	Término referente a la capacidad de diferentes redes para comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.
IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.
ISDN	Red pública utilizada para transmitir varios tipos de información, texto, imágenes, sonido, etcétera.
ISO	Organización que especifica estándares de calidad internacionales.
ISO 9000	Juego de normas de calidad internacional que unifica el control de calidad a nivel mundial.
ISO 9001	Modelo de calidad para empresas de diseño, fabricación e instalación de equipo.
ISO 9002	Modelos de aseguramiento de calidad y satisfacción del cliente en el producto final.
Kernel	Parte del sistema operativo que actúa directamente con el hardware al más bajo nivel.
Kilobyte	KB. 1024 bytes.
Láser	Tecnología de semiconductores que permite concentrar la luz en un solo punto mediante señales electrónicas. Utilizada en tecnologías de impresión.
Layer	En el lenguaje de redes se refiere a cada uno de los subsistemas que interactúan en los procesos de la red.
LED	Tecnología electrónica que permite emitir luz imitando estados binarios 1=luz, 0=apagado.
Link	Término utilizado para referirse a los componentes lógicos y físicos que permiten la comunicación entre dos sistemas.
LLC	Controla las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI).
Login	Proceso de entrada a la red utilizado como término para indicar que la estación está dentro de la red.
Logon	Proceso de entrada a un host. Utilizado para indicar que en realidad el trabajo se desarrolla en el host.
LPT	Abreviatura para asignar puertos paralelos.
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico.
MAN	Red de Area Metropolitana.
Marcado por pulsos	Técnica utilizada para mandar la señal del número

	telefónico al que queremos contactar mediante cambios de intensidad en el voltaje.
Marcado por tonos	Técnica utilizada para mandar la señal del número telefónico al que queremos contactar mediante cambios de frecuencia del voltaje.
MAU	Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él asigna quién tiene el Token Passing o derecho de transacción.
Megabyte	MB. 1'048,576 bytes. Formalmente es 1 K de KB.
MIME	Especificación para redes y transmisiones multipunto.
MIT	Cable de par trenzado sin blindaje.
Módem	Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmitibles por vía telefónica.
Motherboard	Tarjeta principal que contiene los lugares donde se alojarán todos los dispositivos físicos de la computadora.
Multimedia	Incorporación de varios tipos de información: sonidos, textos, gráficos, video, etcétera.
Multitasking	Capacidad de un equipo de llevar más de una tarea a la vez.
NetBios	Interface estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
NFS	Sistema de archivos de red. Genéricamente es un sistema que permite el acceso a un servidor de archivos.
Nodo	Estación de trabajo con identificación propia que puede ser fuente y destino en la red.
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.
Output	Salida de datos se llama a los procesos de una computadora que entregan datos a otro dispositivo o directamente al usuario.
Packet	Unidad de información a transmitir. No contiene dirección ni destino, tan sólo ruta (el siguiente punto a llegar).
Partición	Porción específica de un dispositivo dedicado a una determinada tarea y que está organizada como una sola unidad lógica.
Patch Panel	Centro de empalme. Lugar donde llegan todos los cableados para conexión a la infraestructura de red.
Path	Nombre asignado a la variable que nos indica las rutas lógicas de los datos.
PBX	Comúnmente llamado conmutador, es el sistema de intercambio de líneas telefónicas.
PC cards	Dispositivos periféricos que agregan una amplia variedad de posibilidades a las computadoras: almacenamiento, memoria, manejo de periféricos, fax, red, comunicaciones, etc. Existen tres tipos de acuerdo a su tamaño.
PCI	Estándar de bus para periféricos que típicamente utiliza DMS tipo F y Fast IO bidireccional. Desarrollado por Intel.
PCMCIA	Estándar de bus para tarjetas periféricas de computadoras portátiles.
PDN	Redes públicas de conmutación de paquetes.
Peer-to-peer	Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Propietario	Término utilizado en computación para decir que la tecnología utilizada es desarrollada por la marca propia

Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.
Queue	Fila de espera. Grupo de procesos por realizar.
RAID	Arreglo de discos redundante. Juego de discos armado para aumentar la velocidad de lectura/escritura y seguridad de la información. Existen 5 niveles, desde la copia espejo hasta la escritura paralela con redundancia.
RAM	Memoria de lectura y escritura.
RAS	Servicio de acceso remoto a la red.
RDI	Red digital de servicios integrados. Clase de servicios para transmitir varios tipos de información, texto, imágenes, sonido, etcétera, mediante la red pública.
Repetidor	Dispositivo que transmite y amplifica la señal de la red.
RG11	Cable coaxial grueso usado en Ethernet.
RG58	Cable coaxial delgado de 50 ohms usado en Ethernet.
RG62	Cable coaxial delgado de 62 ohms usado en ARCNet.
RJ11	Conector para MIT 2 pares.
RJ45	Conector para MIT 4 pares.
ROM	Memoria de sólo lectura.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
RS232	Interface serial entre DTE y DCE.
SAA	Enfocado a dar conectividad y migración entre sistemas de las aplicaciones.
SAC	Concentrador que en una red FDDI tiene conexión de círculo.
SCSI	Estándar desarrollado para conectar dispositivos periféricos y a microcomputadoras con una velocidad máxima de 5 Mbps. Utiliza cable de 50 hilos.
SDH	El equivalente del comité CCITT para redes ópticas.
SDLC	Estándar en las arquitecturas SNA para transmisiones punto a punto.
Seek time	Tiempo de búsqueda. Intervalo entre la activación de la señal y la llegada de la cabeza al sector.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
Shareware	Software de disponibilidad y evaluación total que se puede encontrar sin costo en la red o en cualquier otro sitio. El pago por dicho software se realiza cuando el programa ha sido evaluado durante un tiempo razonable y el usuario decide utilizarlo de forma permanente. Este sistema se basa en la buena fe del usuario que responsablemente registra su software con su autor sin responsabilidad para el distribuidor del mismo.
Sincronía	Forma de transmisión de datos donde se necesita señal adicional de reloj para que el transmisor y el receptor funcionen a la misma velocidad.
SLIP	Protocolo para TCP/IP vía serial.
SNA	Arquitectura de protocolos para redes.
SNMP	Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.
SPX	Trabaja en el cuarto nivel de OSI. Brinda apoyo a IPX garantizando la llegada y controlando las secuencias.
SQL	El lenguaje de consulta a la base de datos cliente/servidor más conocido.
STP	Cable de par trenzado con blindaje o aislamiento magnético.

Wireless terminals and
Information Appliances
Wireless LANs, Tablets and PDAs

Business Offices

Remote
Computing

Web
Computing

Web-Platform
Desktop





Supervisor	Usuario de la red con autoridad para realizar las tareas de alto nivel de cliente-servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman administrador.
T1	Línea de transmisión implementada por AT&T con velocidad de 1.544 Mbps.
T3	Servicio de transmisión de datos que opera a 45 Mbps.
TCP/IP	Protocolos definidos por catadráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.
TELNET	Utería de TCP/IP que permite un logon remoto sobre un host.
Terminador	Componente del cableado que empata la impedancia característica del cable para regular las señales eléctricas en la red.
Tiempo de acceso	Intervalo entre el tiempo de una solicitud de datos por el sistema y el tiempo en que el dispositivo los tiene disponibles.
Token Passing	Estafeta. Método de comunicación en red en el que cada elemento debe recibir el permiso para hablar o la estafeta.
Token Ring	Red local en la que el permiso para transmitir es secuencial o en anillo.
Topología	Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.
TP	Cable de pares trenzados.
Transfer rate	Promedio de datos que son enviados y recibidos por un disco duro.
Transciever	Dispositivo de Ethernet que permite el cambio de medio físico a cable.
UPS	Fuente de poder que se activa cuando la señal de corriente alterna se pierde para evitar que los servidores se apaguen de manera abrupta.
Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red pero no los modifica sustancialmente. Tiene derechos de uso pero no de mantenimiento mayor.
Virtual Circuit	Conexión lograda vía programación que se comporta como si existiera conexión física directa.
WACK	Describe el estado de espera hasta que se recibe confirmación de que la transmisión se realizó con éxito.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.
WEB site de WWW	Servidores de internet que contienen la información disponible para los usuarios de esa red.
X.21	Protocolo usado en las redes telefónicas digitales para voz y datos en transmisión síncrona Full Duplex.
X.25	Protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.
X.28	Estándar para la forma en que las terminales asíncronas tienen acceso a los paquetes de la red y sus comandos.
X.3	Estándar de comunicaciones ANSI.

Wireless Terminals and Information Appliances
Cámpora, L. et al., Tablets and Pagers

Remote Computing

Web Computing

