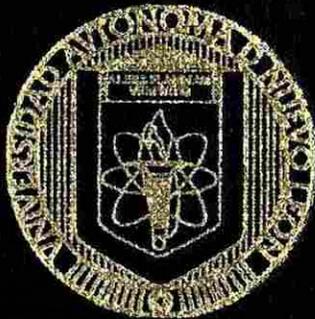


UNIVERSIDAD AUTONOMA DE NUEVO LEON

**FACULTAD DE CONTADURIA PUBLICA
Y ADMINISTRACION**

DIVISION DE ESTUDIOS DE POSTGRADO



**PROYECTO PARA ADQUIRIR EL GRADO
DE MAESTRO EN INFORMATICA ADMINISTRATIVA**

REDES LOCALES UNA VISION GENERAL

H. JURADO

Presidente: M.I.A. JOSE FELIPE RAMIREZ RAMIREZ

Secretario: M.A. FRANCISCO A. CORTEZ CERDA

Vocal: M.I.A. ENRIQUE HERNANDEZ HDZ.

POSTULANTE: L.A. ROBERTO GAITAN MARTOS

TM

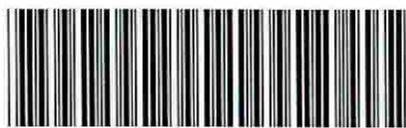
Z7164

.C8

FCPYA

2001

.G34



1020146103



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

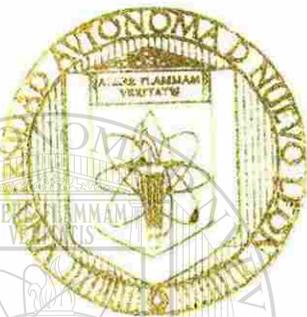


DIRECCIÓN GENERAL DE BIBLIOTECAS

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE CONTADURIA PUBLICA
Y ADMINISTRACION

DIVISION DE ESTUDIOS DE POSTERADO



PROYECTO PARA ADQUIRIR EL GRADO
DE MAESTRO EN INFORMATICA ADMINISTRATIVA

REDES LOCALES UNA VISION GENERAL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DIRECCIÓN GENERAL DE BIBLIOTECAS

Presidente: M.L.A. JOSE FELIPE RAMIREZ RAMIREZ

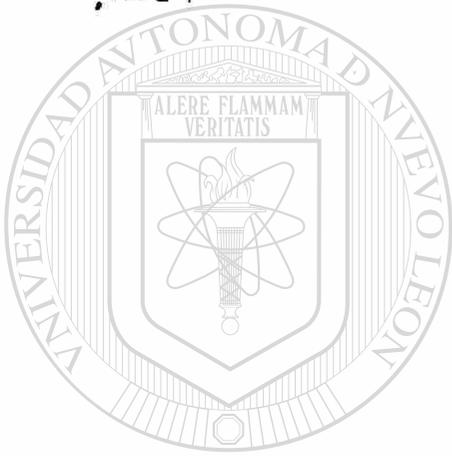
Secretario: M.A. FRANCISCO A. CORTEZ CERDA

Vocal: M.L.A. ENRIQUE HERNANDEZ HDZ.

POSTULANTE: L.A. ROBERTO GAITAN MARTOS

970749

TH
Z7164
.C8
T074A
2001
.G34



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

®

DIRECCIÓN GENERAL DE BIBLIOTECAS

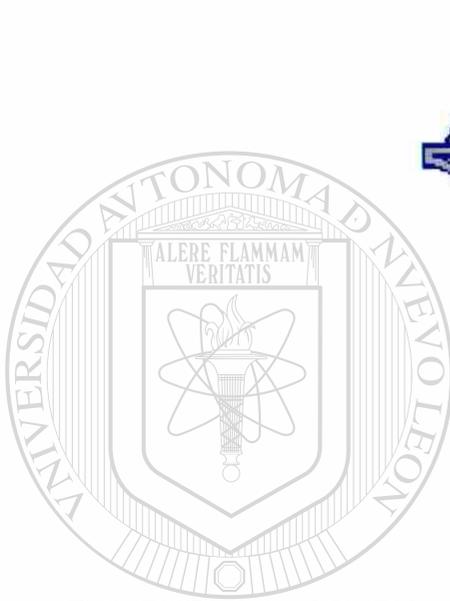


FONDO
TESIS

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

**FACULTAD DE CONTADURÍA PÚBLICA Y
ADMINISTRACIÓN**

DIVISIÓN DE ESTUDIOS DE POSGRADO



**PROYECTO PARA ADQUIRIR EL GRADO DE MAESTRO
EN INFORMÁTICA ADMINISTRATIVA**

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

“REDES LOCALES, UNA VISIÓN GENERAL”

JURADO:

PRESIDENTE: M.I.A. JOSÉ FELIPE RAMIREZ RAMIREZ.

SECRETARIO: M.A. FRANCISCO A. CORTÉZ CERDA.

VOCAL: M.I.A. ENRIQUE HERNANDEZ HERNANDEZ.

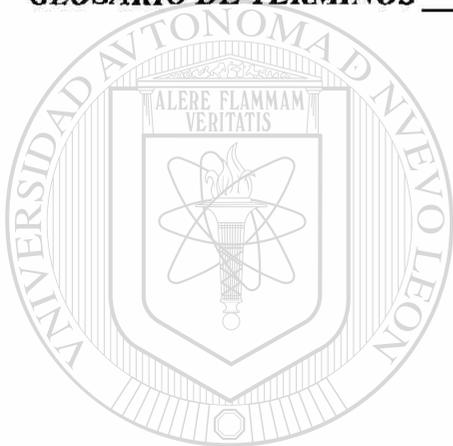
POSTULANTE: L.A. ROBERTO GAITAN MARTOS

CONTENIDO

CONTENIDO	1
DEDICATORIAS Y AGRADECIMIENTOS	4
INTRODUCCIÓN A LAS REDES LOCALES	5
COMPARTIR ARCHIVOS	5
IMPRESIÓN EN RED	5
APLICACIONES DE RED	6
APLICACIONES CLIENTE/SERVIDOR	6
ACCESO A INTERNET	7
VISTA RÁPIDA AL MODELO OSI DE ISO	7
SISTEMA DISTRIBUIDO Y RED LOCAL	8
REDES DE COMUNICACIONES	8
REDES CONMUTADAS	9
CONMUTACIÓN DE PAQUETES	9
CONMUTACIÓN DE CIRCUITOS	9
REDES DE DIFUSIÓN	10
CÓMO FUNCIONA UNA RED	10
TOPOLOGÍA DE UNA RED	11
ESTÁNDARES APLICABLES A LAS REDES LAN (IEEE)	11
TOPOLOGÍA FÍSICA	13
TOPOLOGÍA LÓGICA	13
TOPOLOGÍA EN BUS	13
TOPOLOGÍA EN ANILLO	14
TOPOLOGÍA EN ESTRELLA	15
TOPOLOGÍA EN ESTRELLA PASIVA	16
TOPOLOGÍA DE ESTRELLA ACTIVA	16
TOPOLOGÍAS LÓGICAS	16

TOPOLOGÍA ANILLO-ESTRELLA	16
TOPOLOGÍA BUS-ESTRELLA	18
INTERCONEXIÓN DE REDES	18
CONCEPTO DE SEGMENTO	20
SEGMENTACIÓN: SUS NECESIDADES	20
HUBS (CONCENTRADORES)	23
REPETIDORES	24
BRIDGES (PUENTES)	24
ROUTER (ENCAMINADOR)	25
GATEWAYS (PASARELAS)	26
ELEMENTOS DE UNA RED	26
TARJETAS DE INTERFAZ DE RED	26
DETERMINACIÓN DE LA VELOCIDAD DE TRANSMISIÓN EN UNA RED	27
MEDIOS DE TRANSMISIÓN DE UNA RED LOCAL	28
CABLES	28
PAR TRENZADO	28
CABLE COAXIAL	29
CABLE DE FIBRA ÓPTICA	31
MEDIOS INALÁMBRICOS	33
ENLACES ÓPTICOS AL AIRE LIBRE	33
MICROONDAS	34
LUZ INFRARROJA	34
SEÑALES DE RADIO	35
COMUNICACIONES VIA SATELITE	35
CABLEADO ESTRUCTURADO	37
TOPOLOGÍAS EN EL CABLEADO ESTRUCTURADO	37
ESTÁNDARES	38
NORMATIVAS PARA EL CABLEADO ESTRUCTURADO	38
CABLES: TIPOS DE CABLES EN EL CABLEADO ESTRUCTURADO	38
PROTOCOLO TCP/IP	39
CARACTERÍSTICAS DE TCP/IP	39
FUNCIONAMIENTO DE TCP/IP	39
PROTOCOLO IP	39
DIRECCIONAMIENTO IP	40
MÁSCARA DE SUBRED	40
DIRECCIONES UTILIZADAS	41
RELACION ENTRE DIRECCIONES IP Y DIRECCIONES FÍSICAS	42

PROCOLO TCP	42
SISTEMAS OPERATIVOS DE RED	42
ACCESO REMOTO A LA RED LOCAL	43
INTRANET	44
SOFTWARE DE INTRANETS	44
CORTAFUEGOS (FIREWALL)	44
GROUPWARE	44
CONCLUSIONES	46
GLOSARIO DE TÉRMINOS	48



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

DEDICATORIAS Y AGRADECIMIENTOS

A MI PADRE, POR DARME EL EJEMPLO DE VALORAR LAS COSAS VERDADERAMENTE IMPORTANTES.

A MI MADRE, POR DARME LA CERTEZA DE SABER QUE SIEMPRE SEGUIRÁS ESTANDO CONMIGO.

A JOSÉ ROMÁN, ALEJANDRO Y SAIRA POR EL CARIÑO Y APOYO QUE SIEMPRE ME HAN MANIFESTADO.

A YOLANDA, POR PERMITIRME LA DICHA DE FORJAR A TU LADO MI PROPIA FAMILIA.

A MIS AMIGOS, POR SUS CONSEJOS Y COMPAÑÍA.

A MIS MAESTROS POR SU GUIA EN EL CAMINO DEL CONOCIMIENTO.

A DIOS, POR EL SOLO HECHO DE PRESTARME LA VIDA.

INTRODUCCIÓN A LAS REDES LOCALES

Lo primero que se puede preguntar un usuario cuando se plantea la posibilidad de instalación o utilización de una red local, es saber cómo va a mejorar su trabajo en la computadora al utilizar dicho entorno. La respuesta va a ser diferente según el tipo de trabajo que desempeñe. En resumen, una red local proporciona la facilidad de compartir recursos entre sus usuarios. Esto es:

- Supone compartir archivos.
- Supone compartir impresoras.
- Se pueden utilizar aplicaciones específicas de red.
- Se pueden aprovechar las prestaciones cliente/servidor.
- Se puede acceder a sistemas de comunicación global.

COMPARTIR ARCHIVOS

La posibilidad de compartir archivos es la función principal de las redes locales. La aplicación básica consiste en utilizar archivos de otros usuarios, sin necesidad de utilizar un disquete.

La ventaja fundamental es la de poder disponer de directorios en la red a los que tengan acceso un grupo de usuarios, y en los que se puede guardar la información que comparten dichos grupos.

Ejemplo: se crea una carpeta para el departamento de contabilidad, otra para el departamento de ventas y otra para el departamento de diseño, facilita que estos usuarios tengan acceso a la información que les interesa de forma instantánea. Si a esto se añaden aplicaciones concretas, entonces el trabajo en grupo mejora bastante con la instalación de la red local. Esto se aprecia en las aplicaciones de bases de datos preparadas para el trabajo en redes locales (la mayoría de las actuales), lo que permite que varios usuarios puedan acceder de forma simultánea a los registros de la base de datos, y que las actualizaciones que realice un operador queden inmediatamente disponibles para el resto de los usuarios.

IMPRESIÓN EN RED

Las redes locales permiten que sus usuarios puedan acceder a impresoras de calidad y alto precio sin que suponga un desembolso prohibitivo. Por ejemplo, si tenemos una oficina en la que trabajan siete personas, y sus respectivos ordenadores no están conectados mediante una red local, o compramos una impresora para cada usuario (en total siete), o que cada usuario grabe en un disquete su documento a imprimir y lo lleve donde se encuentra la impresora. Si hay instalada una red local, lo que se puede hacer es comprar una o dos impresoras de calidad, instalarlas y que los usuarios las compartan a través de la red.

Cuando se comparte una impresora en la red, se suele conectar a un ordenador que actúa como servidor de impresión, y que perfectamente puede ser el equipo de un usuario. También existen impresoras que disponen de una tarjeta de red que permite la conexión directa en cualquier punto de la red sin necesidad de situarse cerca de un servidor.

Algo complementario a la impresión en red es la posibilidad de compartir dispositivos de fax. Si una computadora tiene configurado un módem para utilizarlo como fax, puede permitir que el resto de los usuarios de la red lo utilicen para enviar sus propios documentos.

APLICACIONES DE RED

Existe un gran número de aplicaciones que aprovechan las redes locales para que el trabajo sea más provechoso. El tipo de aplicaciones más importante son los programas de correo electrónico. Un programa de correo electrónico permite el intercambio de mensajes entre los usuarios. Los mensajes pueden consistir en texto, sonido, imágenes, etc. y llevar asociados cualquier tipo de archivos. En cierto modo el correo electrónico llega a sustituir a ciertas reuniones y además permite el análisis más detallado del material que el resto de usuarios nos remitan.

APLICACIONES CLIENTE/SERVIDOR

Es un concepto muy importante en las redes locales para aplicaciones que manejan grandes volúmenes de información. Son programas que dividen su trabajo en dos partes, una parte cliente que solicita un determinado trabajo en la computadora del usuario y otra parte servidor que gestiona dicho trabajo con dos finalidades principales:

- Disminuir la carga de trabajo del cliente.
- Reducir el tráfico de la red.

Ejemplo: si disponemos de una computadora que actúe como servidor de base de datos, con un enfoque tradicional, el servidor solamente lo es de archivos. Si en algún momento el usuario quiere hacer una selección de personas mayores de 30 años por ejemplo, se deben leer todos los registros de la base de datos para comprobar cuáles cumplían la condición. Esto supone un elevado tráfico en la red. Con las aplicaciones cliente/servidor una consulta sobre una base de datos se envía al servidor, quien realiza la selección de registros y envía solo los campos que le interesan al usuario. Se reduce así considerablemente el tráfico en la red y el cliente recibe el trabajo hecho. El sistema en sí resulta bastante más rápido, aunque a cambio requiere que los servidores tengan mayores capacidades.

ACCESO A INTERNET

Es una de las funciones que con el tiempo han adquirido mucha relevancia en el trabajo mediante el uso de computadoras. Consiste en la posibilidad de configurar un CPU (unidad central de procesamiento) con una conexión permanente a servicios en línea externos, de forma que los usuarios de la intranet no necesiten utilizar un módem personal para acceder a ellos. El ejemplo más de moda es el acceso a Internet.

Mediante un servidor de comunicaciones se puede mantener una línea permanente de alta velocidad que enlace la intranet con Internet. El servidor puede estar equipado con un módem o una tarjeta de comunicación, que activa la conexión cuando algún usuario de la red lo necesita. Cuando la conexión está activa, cualquier otro usuario puede compartirla, aunque en este caso las capacidades de cada usuario, como la velocidad de transmisión, serán menores que si tuvieran una conexión individual.

VISTA RÁPIDA AL MODELO OSI DE ISO

OSI : Open System Interconnections: fue creado a partir del año 1978, con el fin de conseguir la definición de un conjunto de normas que permitieran interconectar diferentes equipos, posibilitando de esta forma la comunicación entre ellos. El modelo OSI fue aprobado en 1983.

Un sistema abierto, que es el que permite el intercambio de información al interior y al exterior del mismo, debe cumplir las normas que facilitan la interconexión tanto a nivel hardware como software con otros sistemas con arquitecturas distintas.

Este modelo define los servicios y los protocolos que posibilita la comunicación, dividiéndolos en 7 niveles diferentes, en el que cada nivel se encarga de problemas de distinta naturaleza interrelacionándose con los niveles contiguos, de forma que cada nivel se abstrae de los problemas que los niveles inferiores solucionan, para dar solución a un nuevo problema, del que se abstraerán a su vez los niveles superiores.

NIVELES	FUNCIÓN	EJEMPLO
Aplicación	Semántica de los datos	Programa de Correo Electrónico
Presentación	Representación de los datos	HTTP (Hipertext Transfer Protocol)
Sesión	Diálogo ordenado	Gateways
Transporte	Extremo a extremo	TCP (Transmission Control Protocol)
Red	Encaminamiento	IP (Internet Protocol), ruter
Enlace	Punto a punto	HDLC o ADCCP, bridge
Físico	Eléctrico/Mecánico	Cableado

Se puede decir que la filosofía de este modelo se basa en la idea de dividir un problema grande (la comunicación en sí), en varios problemas pequeños, independizando cada problema del resto. Es un método parecido a las cadenas de montaje de las fábricas.; los niveles implementan a un grupo de operarios de una cadena, y cada nivel, al igual que en la cadena de montaje, supone que los niveles anteriores han solucionado unos problemas de los que él se abstraerá para dar solución a unos nuevos problemas, de los que se abstraerán los niveles superiores.

SISTEMA DISTRIBUIDO Y RED LOCAL

No se debe confundir una red local con un sistema distribuido. Aunque parezca que son conceptos similares difieren en algunas cosas.

Un sistema distribuido es multiusuario y multitarea. Todos los programas que se ejecuten en un sistema distribuido lo van a hacer sobre el CPU del servidor en lo que en términos informáticos se denomina "tiempo compartido". Un sistema distribuido comparte un CPU.

Sin embargo, en una intranet, lo que en realidad se denomina servidor, lo es, pero de archivos o de bases de datos. Cada usuario tendrá una PC (Personal Computer O Computadora Personal) autónoma con su propio CPU dónde se ejecutarán las aplicaciones que correspondan. Además, con la aparición de la arquitectura cliente/servidor, el CPU del servidor puede ejecutar algún programa que el usuario solicite.

Una red local puede tener distintas configuraciones que se verán más adelante, pero básicamente se pueden hablar de dos tipos:

- **Red con un servidor:** existe un servidor central que es el "motor" de la red. El servidor puede ser activo o pasivo dependiendo del uso que se le dé.
- **Peer to peer :** una red de igual a igual. Todos los CPU de la red pueden hacer la función de servidor y de cliente.

REDES DE COMUNICACIONES

Dependiendo de su arquitectura y de los procedimientos empleados para transferir la información las redes de comunicación se clasifican en :

- Redes conmutadas
- Redes de difusión

REDES CONMUTADAS

Consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión (cables), formando la mayoría de las veces una topología de malla, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios. Una transmisión de este tipo tiene 3 fases :

- Establecimiento de la conexión.
- Transferencia de la información.
- Liberación de la conexión.

Se entiende por conmutación en un nodo, a la conexión física o lógica, de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información que llegue por el primer camino al segundo. Un ejemplo de redes conmutadas son las redes de área extensa (WAN).

Las redes conmutadas se dividen en :

- Conmutación de paquetes.
- Conmutación de circuitos.

CONMUTACIÓN DE PAQUETES

Se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro, la divide en paquetes. Cada paquete es enviado por el medio con información que lo identifica de los paquetes subsecuentes. En cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo. Otras características importantes de su funcionamiento son :

- En cada nodo intermedio se apunta una relación de la forma : “todo paquete con origen en el nodo A y destino en el nodo B tiene que salir por la salida 5 de mi nodo”.
- Los paquetes se numeran para poder saber si se ha perdido alguno en el camino.
- Todos los paquetes de una misma transmisión viajan por el mismo camino.
- Pueden utilizar parte del camino establecido más de una comunicación de forma simultánea.

CONMUTACIÓN DE CIRCUITOS

Es el procedimiento por el que dos nodos se conectan, permitiendo la utilización de forma exclusiva del circuito físico durante la transmisión. En cada nodo intermedio de la red se cierra un circuito físico entre un cable de entrada y una salida de la red. La red telefónica es un ejemplo de conmutación de circuitos.

REDES DE DIFUSIÓN

En este tipo de redes no existen nodos intermedios de conmutación; todos los nodos comparten un medio de transmisión común, por el que la información transmitida por un nodo es conocida por todos los demás. Ejemplo de redes de difusión son :

- Comunicación por radio.
- Comunicación por satélite.
- Comunicación en una red local.

CÓMO FUNCIONA UNA RED

Se puede pensar por un momento en el servicio de correos. Cuando alguien desea mandar una carta a otra persona, la escribe, la mete en un sobre con el formato impuesto por correos, le pone un sello y la introduce en un buzón; la carta es recogida por el cartero, clasificada por el personal de correos, según su destino y enviada a través de medios de transporte hacia la ciudad destino; una vez allí otro cartero irá a llevarla a la dirección indicada en el sobre; si la dirección no existe, al cabo del tiempo la carta devolverá al origen por los mismos cauces que llegó al supuesto destino.

Más o menos, esta es la forma en que funciona una red: la carta escrita es la información que se quiere transmitir; el sobre y sello es el paquete con el formato impuesto por el protocolo que se utiliza en la transmisión; la dirección del destinatario es la dirección del nodo destino y la dirección del remitente, será la dirección del nodo origen, los medios de transporte que llevan la carta cerca del destino es el medio de transmisión (cable coaxial, fibra óptica, etc.); las normas del servicio de correos, carteros y demás personal son los protocolos de comunicaciones establecidos.

Si se supone que se está utilizando el modelo OSI de la ISO. Este modelo tiene 7 niveles, mencionados anteriormente, es como decir que la carta escrita pasa por 7 filtros diferentes (trabajadores con diferentes cargos) desde que la ponemos en el buzón hasta que llega al destino. Cada nivel de esta torre se encarga de realizar funciones diferentes en la información a transmitir. Cada nivel por el que pasa la información a transmitir que se ha insertado en un paquete, añade información de control, que el mismo nivel en el nodo destino irá eliminando. Además se encarga de cosas muy distintas: desde el control de errores, hasta la reorganización de la información transmitida cuando esta se ha fragmentado en tramas o paquetes.

Si la información va dirigida a una red diferente (otra ciudad en el caso de la carta), la trama o paquete debe llegar a un dispositivo de interconexión de redes (router, gateway, bridges), que decidirá, dependiendo de su capacidad, el camino que debe seguir la trama o paquete. Por eso es imprescindible que el paquete lleve la dirección destino y que esta contenga, además de la dirección que identifica al nodo, la dirección que identifica la red a la que pertenece el nodo.

TOPOLOGÍA DE UNA RED

La topología de una red define únicamente la distribución del cable que interconecta las diferentes computadoras, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son :

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El costo que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad o posibilidad de crecer.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba :

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

Estándares aplicables a las Redes LAN (IEEE)

El Comité 802, o proyecto 802, del *Instituto de Ingenieros en Eléctrica y Electrónica* (IEEE) definió los estándares de redes de área local (LAN). La mayoría de los estándares fueron establecidos por el Comité en los 80's cuando apenas comenzaban a surgir las redes entre computadoras personales.

Muchos de los siguientes estándares son también Estándares ISO 8802. Por ejemplo, el estándar 802.3 del IEEE es el estándar ISO 8802.3.

802.1 Definición Internacional de Redes. Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única. Los vendedores de tarjetas de interface de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE. Cada

vendedor es entonces responsable de crear una dirección única para cada uno de sus productos.

802.2 Control de Enlaces Lógicos. Define el protocolo de control de enlaces lógicos (LLC, Logic Link Control) del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación. La capa de Datos-Enlace en el protocolo OSI esta subdividida en las subcapas de Control de Acceso a Medios (MAC, Media Access Control) y de Control de Enlaces Lógicos (LLC, Logic Link Control). En los puentes, estas dos capas sirven como un mecanismo de switcheo modular. El protocolo LLC es derivado del protocolo de Alto nivel para Control de Datos-Enlaces (HDLC, High Level Data Link Control) y es similar en su operación. Nótese que el LLC provee las direcciones de Puntos de Acceso a Servicios (SAP, Service Access Point), mientras que la subcapa MAC provee la dirección física de red de un dispositivo. Las SAP's son específicamente las direcciones de una o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

El LLC provee los siguientes servicios:

- Servicio orientado a la conexión, en el que una sesión es empezada con un Destino, y terminada cuando la transferencia de datos se completa. Cada nodo participa activamente en la transmisión, pero sesiones similares requieren un tiempo de configuración y monitoreo en ambas estaciones.
- Servicios de reconocimiento orientado a conexiones. Similares al anterior, del que son reconocidos los paquetes de transmisión.
- Servicio de conexión sin reconocimiento. En el cual no se define una sesión. Los paquetes son puramente enviados a su destino. Los protocolos de alto nivel son responsables de solicitar el reenvío de paquetes que se hayan perdido. Este es el servicio normal en redes de área local (LAN's), por su alta confiabilidad.

802.3 Redes CSMA/CD. El estándar 802.3 del IEEE (ISO 8802-3), que define cómo opera el método de Acceso Múltiple con Detección de Colisiones (CSMA/CD, Carrier Sense Multiple Access / Collision Detection) sobre varios medios. El estándar define la conexión de redes sobre cable coaxial, cable de par trenzado, y medios de fibra óptica. La tasa de transmisión original es de 10 Mbits/seg, pero nuevas implementaciones transmiten arriba de los 100 Mbits/seg calidad de datos en cables de par trenzado.

802.4 Redes Token Bus. El estándar token bus define esquemas de red de anchos de banda grandes, usados en la industria de manufactura. Se deriva del Protocolo de Automatización de Manufactura (MAP, Manufacturing Automation Protocol). La red implementa el método token-passing para una transmisión bus. Un token es pasado de una estación a la siguiente en la red y la estación puede transmitir manteniendo el token. Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionar la posición física del nodo como se hace en una red token ring. El estándar no es ampliamente implementado en ambientes LAN.

802.5 Redes Token Ring. También llamado ANSI 802.1-1985, define los protocolos de acceso, cableado e interface para la LAN token ring. IBM hizo popular este estándar. Usa un método de acceso de paso de tokens y es físicamente conectada en topología estrella, pero lógicamente forma un anillo. Los nodos son conectados a una unidad de acceso central (concentrador) que repite las señales de una estación a la siguiente. Las unidades de acceso son conectadas para expandir la red, que amplía el anillo lógico. La Interface de Datos en Fibra Distribuida (FDDI, Fiber Distributed Data Interface) fue basada en el protocolo token ring 802.5, pero fue desarrollado por el Comité de Acreditación de Estándares (ASC) X3T9.

Es compatible con la capa 802.2 de Control de Enlaces Lógicos y por consiguiente otros estándares de red 802.

TOPOLOGÍA FÍSICA

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topología físicas puras :

- Topología en anillo.
- Topología en bus.
- Topología en estrella.

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por mas de una topología física.

TOPOLOGÍA LÓGICA

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas :

- Topología anillo-estrella : implementa un anillo a través de una estrella física.
- Topología bus-estrella : implementa una topología en bus a través de una estrella física.

TOPOLOGÍA EN BUS

Consta de un único cable que se extiende de un ordenador al siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada **terminador**, que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus.

Sus principales ventajas son :

- Fácil de instalar y mantener.
- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperantes a todas las estaciones.

Sus principales inconvenientes son :

- Si se rompe el cable en algún punto, la red queda inoperante por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unir las todas a través de un bus troncal.

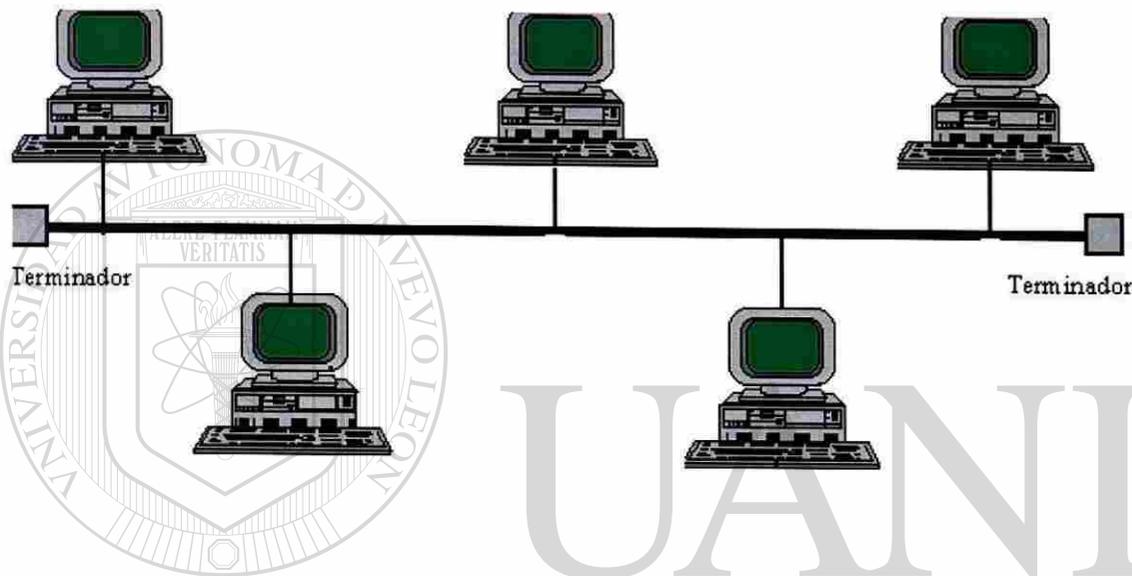


Figura: topología en forma de bus

TOPOLOGÍA EN ANILLO

Sus principales características son:

- El cable forma un bucle o círculo cerrado formando un anillo.
- Todos los CPU que forman parte de la red se conectan a ese anillo.
- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo "paso de testigo".

Los principales inconvenientes serían:

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento.

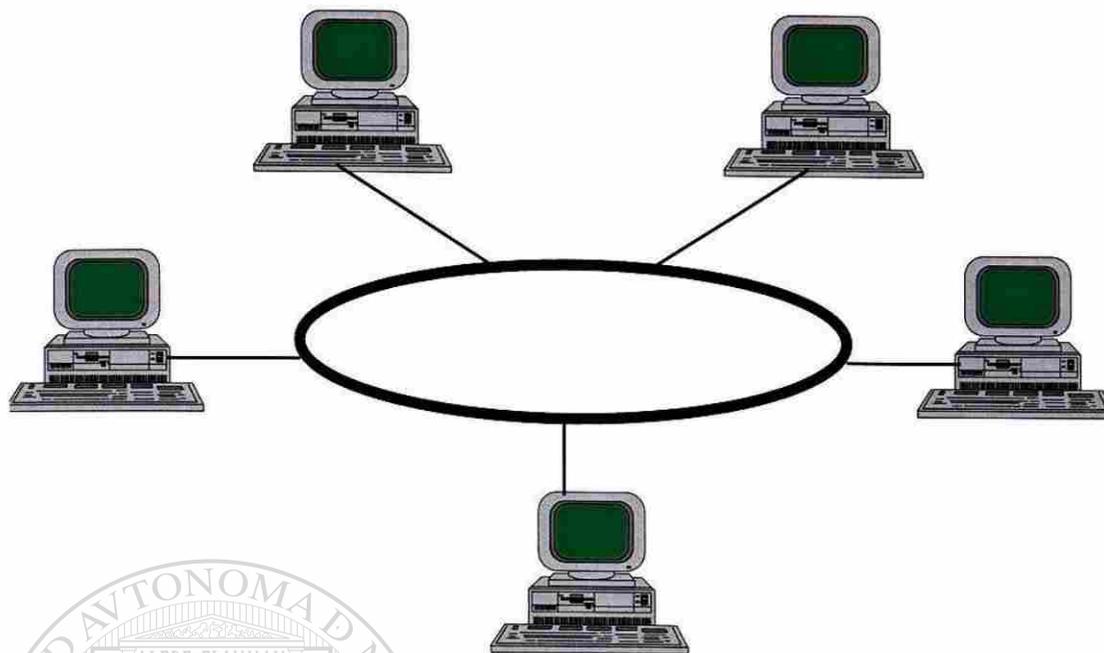
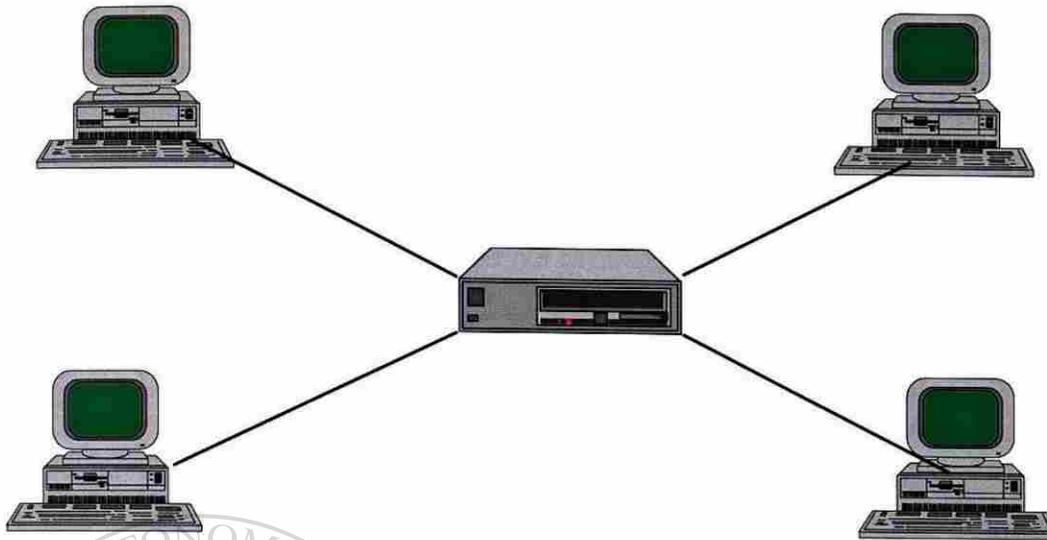


Figura: Topología en anillo

TOPOLOGÍA EN ESTRELLA

Sus principales características son:

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.
- Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio pooling, siendo el nodo central el que se encarga de implementarlo.
- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.
- Existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.
- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
- Este tipo de topología se utiliza cuando el paso de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
- Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
- Es fácil de detectar y de localizar un problema en la red.



TOPOLOGÍA EN ESTRELLA PASIVA

Se trata de una estrella en la que el punto central al que van conectados todos los nodos es un concentrador (hub) pasivo, es decir, se trata únicamente de un dispositivo con muchos puertos de entrada.

TOPOLOGÍA DE ESTRELLA ACTIVA

Se trata de una topología en estrella que utiliza como punto central un hub activo o bien un ordenador que hace las veces de servidor de red. En este caso, el hub activo se encarga de repetir y regenerar la señal transferida e incluso puede estar preparado para realizar estadísticas del rendimiento de la red. Cuando se utiliza un ordenador como nodo central, es éste el encargado de gestionar la red, y en este caso suele ser además del servidor de red, el servidor de archivos.

TOPOLOGÍAS LÓGICAS

TOPOLOGÍA ANILLO-ESTRELLA

Uno de los inconvenientes de la topología en anillo era que si el cable se rompía toda la red quedaba inoperante; con la topología mixta anillo-estrella, éste y otros problemas quedan resueltos.

Las principales características son:

- Cuando se instala una configuración en anillo, el anillo se establece de forma lógica únicamente, ya que de forma física se utiliza una configuración en estrella.
- Se utiliza un concentrador, o incluso un servidor de red como dispositivo central, de esta forma, si se rompe algún cable sólo queda inoperante el nodo que conectaba, y los demás pueden seguir funcionando.
- El concentrador utilizado cuando se está utilizando esta topología se denomina MAU (*Multistation Access Unit o Unidad de Acceso Multiestación*), que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.
- A simple vista, la red parece una estrella, aunque internamente funciona como un anillo.
- Cuando la MAU detecta que un nodo se ha desconectado (por haberse roto el cable, por ejemplo), puentea su entrada y su salida para así cerrar el anillo.

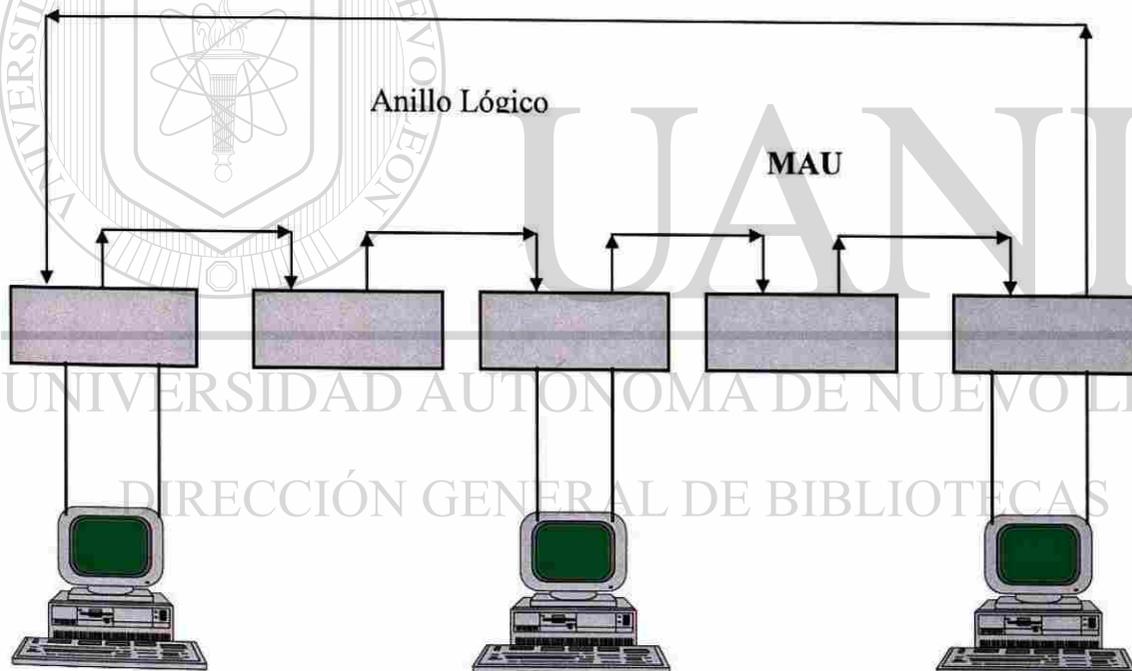


Figura: topología anillo-estrella

TOPOLOGÍA BUS-ESTRELLA

Este tipo de topología es en realidad una estrella que funciona como si fuese en bus. Como punto central tiene un concentrador pasivo (hub) que implementa internamente el bus, y al que están conectados todos los ordenadores. La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

INTERCONEXIÓN DE REDES

Hace algunos años era impredecible la evolución que las comunicaciones, en el mundo de la informática, iban a tener, no se podía prever que fuese necesaria la interconexión ya no sólo de varias computadoras sino de cientos de ellas. No basta con tener las computadoras en una sala conectadas, es necesario conectarlas a su vez con las computadoras del resto de las áreas de una empresa, y con el resto de las sucursales de una empresa situadas en distintos puntos geográficos.

La interconexión de redes permite, si se puede decir así, ampliar el tamaño de una red. Sin embargo el término interconexión se utiliza para unir redes independientes, no para ampliar el tamaño de una.

El número de computadoras que componen una intranet es limitado, depende de la topología elegida, (recuérdese que en la topología define el cableado a utilizar) aunque si lo único que se quisiera fuera sobrepasar el número de ordenadores conectados, podría pensarse en simplemente segmentar la intranet. Sin embargo existen otros factores a tener en cuenta.

Cuando se elige la topología que va a tener una red se tienen en cuenta factores, como son la densidad de tráfico que ésta debe soportar de manera habitual, el tipo de aplicaciones que van a instalarse sobre ella, la forma de trabajo que debe gestionar, etc.; esto debe hacer pensar en que, uno de los motivos por el que se crean diferentes topologías es por tanto el uso que se le va a dar a la red. De aquí se puede deducir que en una misma empresa puede hacerse necesaria no la instalación de una única intranet, aunque sea segmentada, sino la implantación de redes independientes, con topologías diferentes e incluso arquitecturas diferentes y que estén interconectadas.

Habitualmente la selección del tipo y los elementos físicos de una red, se ajusta a las necesidades que se tiene; por este motivo pueden encontrarse dentro de un mismo edificio, varias intranets con diferentes topologías, y con el tiempo pueden surgir la necesidad de interconectarlas.

Se puede ver que por diferentes razones se hace necesaria tanto la segmentación como la interconexión de intranets, y que ambos conceptos a pesar de llevar a un punto en común, parten de necesidades distintas.

La tabla siguiente refleja de forma genérica diferentes casos en los que se plantea la necesidad de segmentar y/o interconectar intranets, dando la opción más idónea para cada uno de los casos planteados.

NECESIDAD	SOLUCIÓN
Debido a la necesidad de manejo de aplicaciones que producen un intercambio importante de información aumenta el tráfico en la red; esto lleva a que baje el rendimiento de la misma.	Dividir la red actual en varios segmentos: Segmentar la red.
Se tiene que ampliar el número de nodos o puestos que forman la intranet, pero se necesita mantener el rendimiento de la red	Crear un nuevo segmento de red en el que se pondrán los nuevos nodos e incluso al que se puedan mover nodos, que por disposición física pueda ser conveniente que pertenezcan al nuevo segmento creado en la misma.
Se tiene la necesidad de unir dos intranets exactamente iguales en la empresa	Se puede optar por definir una de ellas como un segmento de la otra y unir las de esta forma; o bien, interconectar las dos intranets con un dispositivo de nivel bajo.
Se tiene la necesidad de unir dos o más redes con diferentes topologías pero trabajando con los mismos protocolos de comunicaciones.	Es necesario la interconexión de ambas redes a través de dispositivos interconectantes de nivel medio
Se tiene la necesidad de unir dos o más redes totalmente diferentes, es decir, de arquitecturas diferentes.	Es necesario la interconexión de ambas redes a través de dispositivos interconectantes de nivel alto.

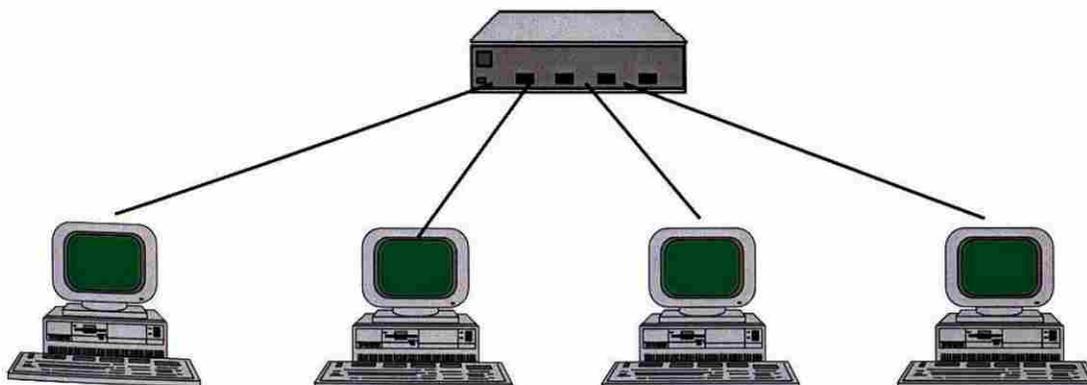


Figura: red inicial con topología lógica en bus y física en estrella a través de un Hub

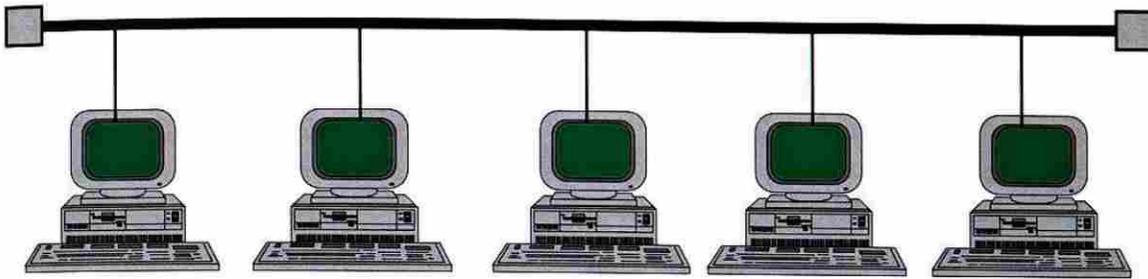


Figura: si se necesita ampliar la red, una solución puede ser esta, pero no mejora el rendimiento de la red porque lógicamente está vista como una única red.

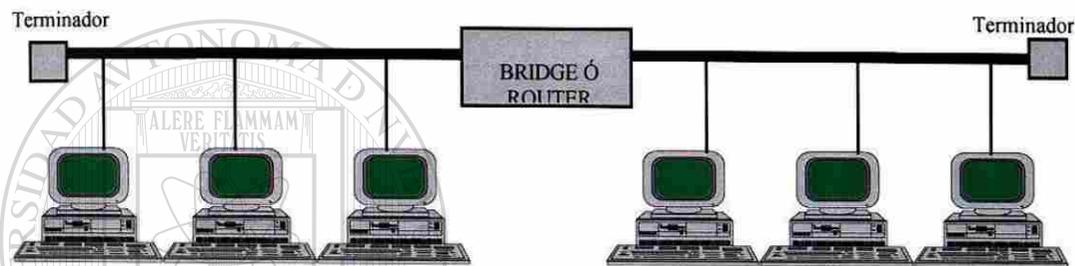


Figura: una solución para ampliar la red puede ser esta, y en esta situación mejora el rendimiento de la red.

CONCEPTO DE SEGMENTO

Un segmento es un bus lineal al que están conectadas varias estaciones y que termina en los extremos. Las características son:

- Cuando se tiene una red grande se divide en trozos, llamados segmentos a cada uno de ellos.
- Para interconectar varios segmentos se utilizan bridges o routers
- El rendimiento de una red aumenta al dividirla en segmentos
- A cada segmento junto a las estaciones a él conectadas se las llama subred

SEGMENTACIÓN: SUS NECESIDADES

Segmentar una intranet consiste en dividirla en subredes para así poder aumentar el número de nodos conectados a ella y/o el rendimiento de la misma.

Cuando se segmenta una intranet, lo que se está haciendo es crear subredes pequeñas que, por decirlo de alguna manera, se autogestionan, de forma que la comunicación entre

segmentos se realiza cuando es necesario, es decir, cuando un nodo de un segmento quiere comunicarse con un nodo del otro segmento; mientras tanto cada segmento de la intranet está trabajando de forma independiente por lo que en una misma intranet se están produciendo varias comunicaciones de forma simultánea; evidentemente esto mejora el rendimiento de la intranet.

La tabla siguiente refleja las longitudes máximas de los segmentos dependiendo de las diferentes topologías de red.

TOPOLOGÍAS	LONGITUD
Ethernet gruesa	500 metros
Ethernet fina	185 metros
Ethernet de par trenzado	100 metros
Ethernet de fibra óptica	2.000 metros
Token-Ring de par trenzado	100 metros

El dispositivo que se utiliza para segmentar una red debe ser inteligente ya que debe ser capaz de decidir hacia qué segmento debe enviar la información llegado a él: si hacia el mismo segmento desde el que la recibió o hacia otro segmento diferente.

Abstrayéndose de algunos detalles, es fácil pensar el segmentar una intranet, ya que se habla de subredes, es como interconectar intranets diferentes. Sin embargo, cuando se habla de segmentar se hace referencia a una única intranet; esto lleva asociado lo siguiente: una única topología, un único tipo de protocolo de comunicaciones, un único entorno de trabajo; cuando se habla de interconectar intranets, en la mayoría de los casos, las intranets tienen como mínimo topologías diferentes. No obstante, debe destacarse que los dispositivos que se utilizan para segmentar redes coinciden con algunos de los dispositivos que son utilizados para interconectar redes diferentes.

Dependiendo del tipo de protocolos que se utilicen en la intranet segmentada, así como de dispositivos que se utilicen para realizar esta segmentación puede hacerse necesario o no el atribuir a cada segmento una dirección de red diferente. Cuando se trabaja con protocolos TCP/IP esto no es necesario, basta con que cada estación tenga su propia dirección IP, y que no aparezcan dos estaciones con la misma dirección, independientemente de si están o no en el mismo segmento de la intranet.

Existen diferentes motivos por los que se puede hacer necesario la segmentación de una intranet, como pueden ser:

- **Necesidad de sobrepasar el número de nodos que la topología permite.** La limitación del número de nodos en una intranet viene impuesta por varios factores, como son el método de acceso al medio que se utiliza, el tipo de cable, el ancho de banda, etc.

- **Mejorar el rendimiento de una intranet en la que ha aumentado el tráfico.** En ocasiones, una intranet que inicialmente funciona bien, con un tiempo de repuesta aceptable, empieza a perder eficiencia; el motivo es claro: de forma paulatina se ha ido incrementando el número de comunicaciones que la intranet debe gestionar, por diferentes motivos como que los usuarios comienzan a conocer la red y la aprovechan más, o que se han ido instalando más aplicaciones.

Existen diferentes formas de atacar este problema: Una de ellas, la más drástica es cambiar algún elemento físico de la intranet: por ejemplo sustituir el cableado que implementa la intranet por uno que pueda soportar velocidades mayores, cambiar las tarjetas de red por otras más rápidas, e incluso cambiar la topología empleada. Una solución menos drástica consiste en segmentar la intranet. Dividirla estratégicamente en dos subredes, reduciendo de esta forma el tráfico en cada una de ellas. Por ejemplo, sobre una intranet inicial repartida por varias aulas de una universidad, se pueden crear subredes por aula, de forma que en cada aula se mejorará el rendimiento de la red.

La interconexión de intranets se puede establecer a varios niveles: desde el nivel físico, a través de un dispositivo llamado Hub (concentrador) hasta niveles más altos (niveles del modelo OSI) a través de dispositivos como un puente (Bridge) o un router (encaminador). La tabla siguiente muestra el nivel en el que trabajan los diferentes dispositivos.

DISPOSITIVO	NIVEL
Repetidor	Físico
Concentrador	Físico
Puente o Bridge	Enlace
Router o Encaminador	Red
Pasarela	Aplicación

Para la segmentación de intranets, y teniendo en cuenta que uno de los motivos por el que se realiza esta operación es mejorar el rendimiento de la red, es necesario emplear dispositivos inteligentes, como pueden ser un encaminador o un puente.

Las redes locales tienen una serie de limitaciones inherentes a su naturaleza:

- Limitaciones en el número de hosts.
- Limitaciones en la distancia que puede cubrir.
- Limitaciones en el número y tipo de nodos que se pueden conectar.
- Limitaciones en el acceso a los nodos.
- Limitaciones en la comunicación con los usuarios.

Para resolver estos problemas se utilizan soluciones de dos naturalezas: software y hardware:

- Elementos de interconexión.
- Software de servicios.

De forma genérica existen varias maneras de ampliar las intranets:

- Hubs: para unir hosts dentro de una red.
- Repetidores: conexión a nivel físico, en el mismo segmento.
- Bridges: conexión a nivel de enlace entre dos segmentos (iguales o distintos).
- Routers: conexión a nivel de red.
- Gateways: conexión a nivel de presentación, entre dos redes distintas.

HUBS (CONCENTRADORES)

Dispositivo que interconecta host dentro de una red. Es el dispositivo de interconexión más simple que existe. Sus principales características son:

- Se trata de una caja de conexiones donde se centralizan todas las conexiones de una red, es decir un dispositivo con muchos puertos de entrada y salida.
- No tiene ninguna función aparte de centralizar conexiones.
- Se suelen utilizar para implementar topologías en estrella física, pero funcionando como un anillo o como un bus lógico.

Hubs activos: permiten conectar nodos a distancias de hasta 609 metros, suelen tener entre 8 y 12 puertos y realizan funciones de amplificación y repetición de la señal. Los más complejos además realizan estadísticas.

Hubs pasivos: son simples cajas de conexiones. Permiten conectar nodos a distancias de hasta 30 metros. Generalmente suelen tener entre 8 y 12 puertos.

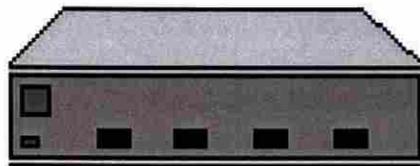
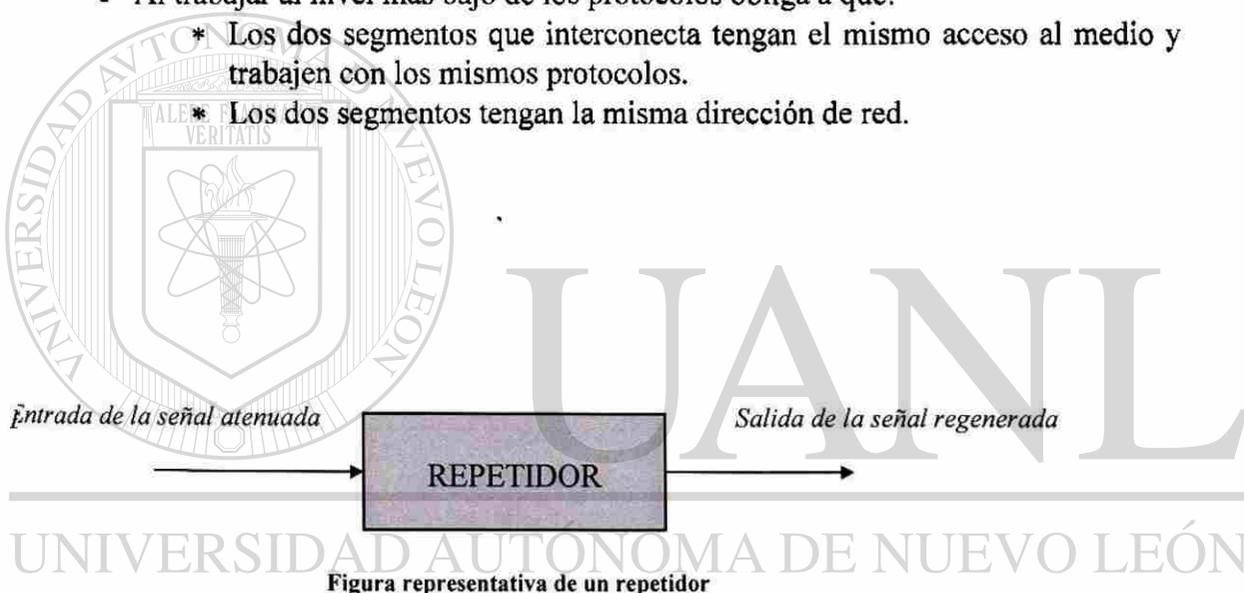


Figura representativa de un HUB

REPETIDORES

Sus principales características son:

- Conectan a nivel físico dos intranets, o dos segmentos de intranet. Hay que tener en cuenta que cuando la distancia entre dos hosts es grande, la señal que viaja por la línea se atenúa y hay que regenerarla.
- Permiten resolver problemas de limitación de distancias en un segmento de intranet.
- Se trata de un dispositivo que únicamente repite la señal transmitida evitando su atenuación; de esta forma se puede ampliar la longitud del cable que soporta la red.
- Al trabajar al nivel más bajo de los protocolos obliga a que:
 - * Los dos segmentos que interconecta tengan el mismo acceso al medio y trabajen con los mismos protocolos.
 - * Los dos segmentos tengan la misma dirección de red.



BRIDGES (PUENTES)

Sus principales características son:

- Son dispositivos que ayudan a resolver el problema de limitación de distancias, junto con el problema de limitación del número de nodos de una red.
- Trabajan al nivel de enlace del modelo OSI, por lo que pueden interconectar redes que cumplan las normas del modelo 802 (3, 4 y 5). Si los protocolos por encima de estos niveles son diferentes en ambas redes, el puente no es consciente, y por tanto no puede resolver los problemas que puedan presentarse.
- Se utilizan para:
 - * Ampliar la extensión de la red, o el número de nodos que la constituyen.
 - * Reducir la carga en una red con mucho tráfico, uniendo segmentos diferentes de una misma red.

- * Unir redes con la misma topología y método de acceso al medio, o diferentes.
- * Cuando un puente une redes exactamente iguales, su función se reduce exclusivamente a direccionar el paquete hacia la subred destino.
- * Cuando un puente une redes diferentes, debe realizar funciones de traducción entre las tramas de una topología a otra.
- Cada segmento de red, o red interconectada con un puente, tiene una dirección de red diferente.
- Los puentes no entienden de direcciones IP, ya que trabajan en otro nivel.
- Los puentes realizan las siguientes funciones:
 - * Reenvío de tramas: constituye una forma de filtrado. Un puente solo reenvía a un segmento a aquellos paquetes cuya dirección de red lo requiera, no traspasando el puente los paquetes que vayan dirigidos a nodos locales a un segmento. Por tanto, cuando un paquete llega a un puente, éste examina la dirección física destino contenida en él, determinado así si el paquete debe atravesar el puente o no.
 - * Técnicas de aprendizaje: los puentes construyen tablas de dirección que describen las rutas, bien sea mediante el examen del flujo de los paquetes (puentado transparente) o bien con la obtención de la información de los “paquetes exploradores” (encaminamiento fuente) que han aprendido durante sus viajes la topología de la red.
- Los primeros puentes requerían que los gestores de la red introdujeran a mano las tablas de dirección.
- Los puentes trabajan con direcciones físicas

ROUTER (ENCAMINADOR)

Sus principales características son:

- Es como un puente incorporando características avanzadas.
- Trabajan a nivel de red del modelo OSI, por tanto trabajan con direcciones IP.
- Un router es dependiente del protocolo.
- Permite conectar redes de área local y de área extensa.
- Habitualmente se utilizan para conectar una red de área local a una red de área extensa.
- Son capaces de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo.
- La forma que tienen de funcionar es la siguiente.
 - * Cuando llega un paquete al router, éste examina la dirección destino y lo envía hacia allí a través de una ruta predeterminada.
 - * Si la dirección destino pertenece a una de las redes que el router interconecta, entonces envía el paquete directamente a ella; en otro caso enviará el paquete a otro router más próximo a la dirección destino.

- * Para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento.
- Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos; para ello incorporan un software que pasa un paquete de un protocolo a otro, aunque no son soportados todos los protocolos.
- Cada segmento de red conectado a través de un router tiene una dirección de red diferente.

GATEWAYS (PASARELAS)

Sus características principales son:

- Se trata de un ordenador u otro dispositivo que interconecta redes radicalmente distintas.
- Trabaja al nivel de aplicación del modelo OSI.
- Cuando se habla de pasarelas a nivel de redes de área local, en realidad se está hablando de routers.
- Son capaces de traducir información de una aplicación a otra, como por ejemplo las pasarelas de correo electrónico.

ELEMENTOS DE UNA RED

Los principales elementos que necesitamos para instalar una red son :

- Tarjetas de interfaz de red o NICs.
- Cable.
- Protocolos de comunicaciones.
- Sistema operativo de red.
- Aplicaciones capaces de funcionar en red.

TARJETAS DE INTERFAZ DE RED

Las tarjetas de interfaz de red (NICs - Network Interface Cards) son adaptadores instalados en un dispositivo, conectándolo de esta forma en red. Es el pilar en el que sustenta toda red local, y el único elemento imprescindible para enlazar dos nodos a buena velocidad (excepción hecha del cable y el software). Existen tarjetas para distintos tipos de redes. Las principales características de una tarjeta de red son:

- Operan a nivel físico del modelo OSI : Las normas que rigen las tarjetas determinan sus características , y sus circuitos gestionan muchas de las funciones de la comunicación en red como:

- * Especificaciones mecánicas: Tipos de conectores para el cable, por ejemplo.
- * Especificaciones eléctricas: definen los métodos de transmisión de la información y las señales de control para dicha transferencia.
- * Método de acceso al medio: es el tipo de algoritmo que se utiliza para acceder al cable que sostiene la red. Estos métodos están definidos por las normas 802.x del IEEE.
- Los circuitos de la tarjeta de red determinan, antes del comienzo de la transmisión de los datos, elementos como velocidad de transmisión, tamaño del paquete, time-out, tamaño de los buffers. Una vez que estos elementos se han establecido, empieza la verdadera transmisión, realizándose una conversión de datos a transmitir a dos niveles :
 - * En primer lugar se pasa de paralelo a serie para transmitirlos como flujo de bits.
 - * Seguidamente se codifican y a veces se comprimen para un mejor rendimiento en la transmisión.
- La dirección física es un concepto asociado a la tarjeta de red : Cada nodo de una red tiene una dirección asignada que depende de los protocolos de comunicaciones que esté utilizando. La dirección física habitualmente viene definida de fábrica, por lo que no se puede modificar. Sobre esta dirección física se definen otras direcciones, como puede ser la dirección IP para redes que estén funcionando con TCP/IP.

DETERMINACIÓN DE LA VELOCIDAD DE TRANSMISIÓN EN UNA RED

Existen varios factores que determinan la velocidad de transmisión de una red, entre ellos podemos destacar :

- El cable utilizado para la conexión. Dentro del cable existen factores como :
 - * El ancho de banda permitido.
 - * La longitud.

Existen otros factores que determinan el rendimiento de la red, son :

- Las tarjetas de red.
- El tamaño del bus de datos de las máquinas.
- La cantidad de retransmisiones que se pueden hacer.

MEDIOS DE TRANSMISIÓN DE UNA RED LOCAL

Se pueden diferenciar dos grupos :

- Los cables.
- Los medios inalámbricos.

CABLES

El cable utilizado para formar una red se denomina a veces *medio*. Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son :

- Velocidad de transmisión que se quiere conseguir.
- Distancia máxima entre nodos que se van a conectar.
- Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

Los cables más utilizados son el par trenzado, el cable coaxial y la fibra óptica.

PAR TRENZADO

Se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no).

Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer.

Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. Está dividido en categorías por el EIA/TIA :

- **Categoría 1:** hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg
- **Categoría 2 :** cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- **Categoría 3 :** velocidad de transmisión de 10 Mbits/seg. Con este tipo de cables se implementa las redes Ethernet 10-Base-T
- **Categoría 4 :** la velocidad de transmisión llega a 16 bits/seg.
- **Categoría 5 :** puede transmitir datos hasta 100 Mbits/seg.

Tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de obra. La mayoría de las mangueras de cable de par trenzado contiene más de un par de hilos por lo que es posible encontrar mangueras ya instaladas con algún par de hilos sin utilizarse. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes.

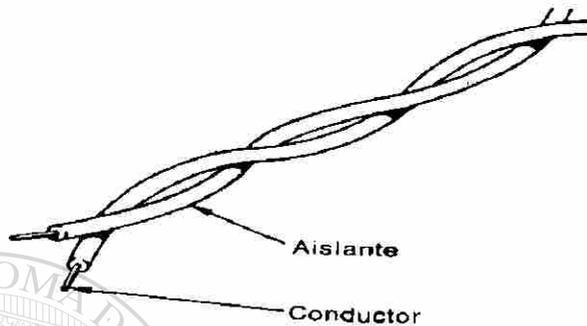


Figura: Cable de par trenzado

CABLE COAXIAL

Consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa está rodeada por una malla metálica que ayuda a bloquear las interferencias; este conjunto de cables está envuelto en una capa protectora. Le pueden afectar las interferencias externas, por lo que ha de estar apantallado para reducir las. Emite señales que pueden detectarse fuera de la red.

Es utilizado generalmente para señales de televisión y para transmisiones de datos a alta velocidad a distancias de varios kilómetros.

La velocidad de transmisión suele ser alta, de hasta 100 Mbits/seg; pero hay que tener en cuenta que a mayor velocidad de transmisión, menor distancia podemos cubrir, ya que el periodo de la señal es menor, y por tanto se atenúa antes.

La nomenclatura de los cables Ethernet tiene 3 partes :

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros de segmento multiplicados por 100.

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión : 10 Mb/seg. Segmentos : máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión : 10 Mb/seg. Segmentos : máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos : máximo de 3600 metros. Velocidad de transmisión : 10 Mb/seg.
100-BASE-X	Fast Ethernet. Velocidad de transmisión : 100 Mb/seg.

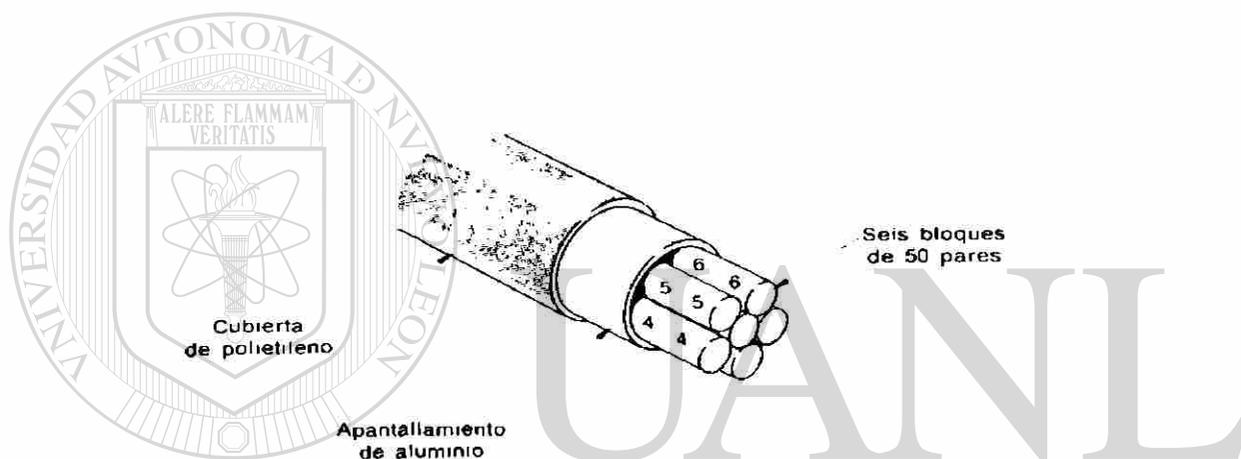


Figura Estructura típica de un cable de pares

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DIRECCIÓN GENERAL DE BIBLIOTECAS

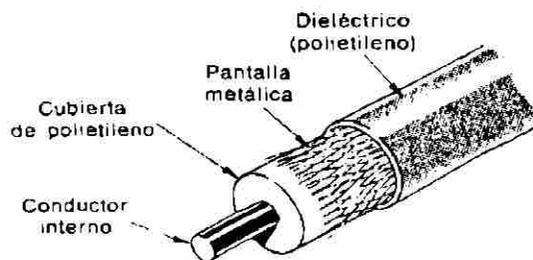


Figura : Estructura típica de un cable coaxial

CABLE DE FIBRA ÓPTICA

Una fibra óptica es un medio de transmisión de la luz que consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura.

En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar éste de un medio a otro que tiene un índice de refracción más pequeño. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra.

Este conjunto está envuelto por una capa protectora. La velocidad de transmisión es muy alta, 10 Mb/seg siendo en algunas instalaciones especiales de hasta 500 Mb/seg, y no resulta afectado por interferencias.

Los cables de fibra óptica tienen muchas aplicaciones en el campo de las comunicaciones de datos:

- Conexiones locales entre ordenadores y periféricos o equipos de control y medición.
- Interconexión de ordenadores y terminales mediante enlaces dedicados de fibra óptica.
- Enlaces de fibra óptica de larga distancia y gran capacidad.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz ($c = 3 \times 10^8$ m/s), mientras que las señales eléctricas recorren los cables a una velocidad entre el 50 y el 80 por ciento de ésta, según el tipo de cable.
- Mayor capacidad de transmisión. Pueden lograrse velocidades por encima de 1 Gbit/s.
- Inmunidad total ante interferencias electromagnéticas. La fibra óptica no produce ningún tipo de interferencia electromagnética y no se ve afectada por rayos o por pulsos electromagnéticos nucleares (NEMP) que acompañan a las explosiones nucleares.
- No existen problemas de retorno de tierra o reflexiones como ocurre en las líneas de transmisión eléctricas.
- La atenuación aumenta con la distancia más lentamente que en el caso de los cables eléctricos, lo que permite mayores distancias entre repetidores.
- Se consiguen tasas de error típicas del orden de 1 en 10^9 frente a las tasas del orden de 1 en 10^6 que alcanzan los cables coaxiales. Esto permite aumentar la velocidad eficaz de transmisión de datos, reduciendo el número de retransmisiones o la cantidad de información redundante necesaria para detectar y corregir los errores de transmisión.

- No existe riesgo de cortocircuito o daños de origen eléctrico.
- Los cables de fibra óptica pesan la décima parte que los cables de corte apantallados. Esta es una consideración de importancia en barcos y aviones.
- Los cables de fibra óptica son generalmente de menor diámetro, más flexibles y más fáciles de instalar que los cables eléctricos.
- Los cables de fibra óptica son apropiados para utilizar en una amplia gama de temperaturas.
- Es más difícil realizar piratería sobre cables de fibra óptica que sobre cables eléctricos. Es necesario cortar la fibra para detectar los datos transmitidos. Las intromisiones sobre fibra óptica pueden detectarse fácilmente midiendo las pérdidas de señal.
- Se puede incrementar la capacidad de transmisión de datos añadiendo nuevos canales que utilicen longitudes de onda distintas de las ya empleadas.
- La fibra óptica presenta una mayor resistencia a los ambientes y líquidos corrosivos que los cables eléctricos.
- Las materias primas para fabricar vidrio son abundantes y se espera que los costos se reduzcan a un nivel similar al de los cables metálicos.
- La vida media operacional y el tiempo medio entre fallos de un cable de fibra óptica son superiores a los de un cable eléctrico.
- Los costos de instalación y mantenimiento para grandes y medias distancias son menores que los que se derivan de las instalaciones de cables eléctricos.

La mayor desventaja es que no se puede insertar fácilmente este cable para conectar un nuevo nodo a la red.

Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación, que consiste en una pérdida de amplitud o intensidad de la señal, lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros.

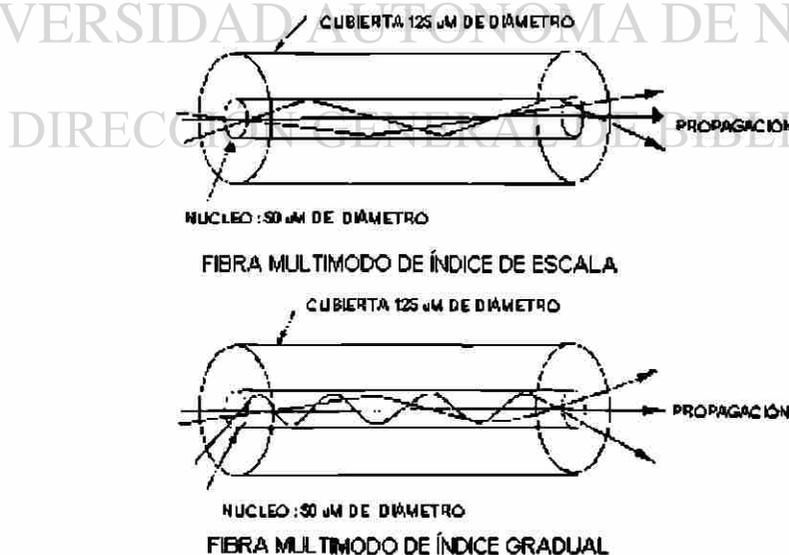
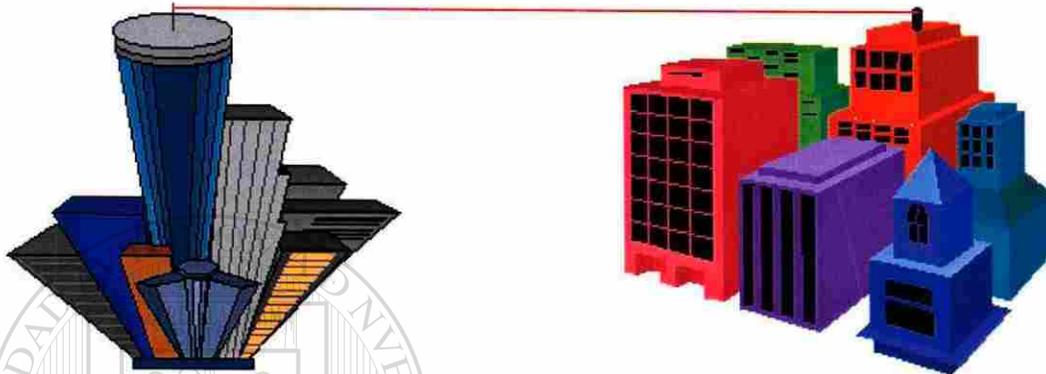


Figura: Propagación multimodo en una fibra óptica de índice de escala y de índice gradual

MEDIOS INALÁMBRICOS

ENLACES ÓPTICOS AL AIRE LIBRE

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire.



El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la línea de visión. Las aplicaciones típicas para estos enlaces se encuentran en los campus de la universidades, donde las carreteras no permiten tender cables, o entre los edificios de una compañía en una ciudad en la que resulte caro utilizar los cables telefónicos.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las potencialidades de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s . El límite para comunicaciones confiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Existen dos efectos atmosféricos importantes a tener en cuenta con los enlaces ópticos al aire libre :

- La dispersión de la luz que atenúa la señal óptica en proporción al número y al tamaño de las partículas en suspensión en la atmósfera. Las partículas pequeñas, como la niebla,

polvo o humo, tienen un efecto que es función de su densidad y de la relación existente entre su tamaño y de la longitud de onda de la radiación infrarroja utilizada. La niebla, con una elevada densidad de partículas, de 1 a 10 μm de diámetro, tienen un efecto más agudo sobre el haz de luz. Las partículas de humo, más grandes, tienen menor densidad y, por tanto, menor efecto.

- Las brisas ascensionales (originadas por movimientos del aire como consecuencia de las variaciones en la temperatura) provocan variaciones en la densidad del aire y, por tanto, variaciones en el índice de refracción a lo largo del haz. Esto da lugar a la dispersión de parte de la luz a lo largo del haz. Este efecto puede reducirse elevando el haz de luz lo bastante con respecto a cualquier superficie caliente o utilizando emisores múltiples. La luz de cada emisor se ve afectada de diferente forma por las brisas, y los haces se promedian en el receptor.

Estos sistemas suelen emplearse para transmisiones digital de alta velocidad en banda base. En Estados Unidos de América, todos los fabricantes de productos láser deben tener una certificación que garantiza la seguridad de sus productos.

MICROONDAS

Los enlaces de microondas se utilizan mucho allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de SHF, de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.

Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2.4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionar hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.

Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que esto ocurra.

LUZ INFRARROJA

Permite la transmisión de información a velocidades muy altas : 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz ; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

SEÑALES DE RADIO

Consiste en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesario la visión directa de emisor y receptor.

La velocidad de transmisión suele ser baja : 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

COMUNICACIONES VIA SATÉLITE

Los satélites artificiales han revolucionado las comunicaciones desde los últimos 20 años. Actualmente son muchos los satélites de comunicaciones que están alrededor de la tierra dando servicio a numerosas empresas, gobiernos, entidades, etc.

Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal ascendiente). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal descendiente). La señal descendiente puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que los canales ascendientes y descendientes se interfieran, ya que trabajan en bandas de frecuencia diferentes.

La capacidad que posee un satélite de recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los gigahertzios. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36000 Km. sobre el ecuador de la tierra. Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

- Existe un retardo de unos 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento "en ocho" de un satélite geoestacionario se necesitan transmisiones frecuentes de tramas de sincronización.
- Los satélites geoestacionarios no son totalmente estacionarios con respecto a la órbita de la tierra. Las desviaciones de la órbita ecuatorial hace que el satélite describa una figura parecida a un ocho (movimiento "en ocho"), de dimensiones proporcionales a la inclinación de la órbita con respecto al ecuador. Estas variaciones en la órbita deben ser corregidas desde una estación de control.

- Los satélites tienen una vida media de siete a diez años, pero pueden sufrir fallos que provocan su salida de servicio. Es, por tanto, necesario disponer de un medio alternativo de servicio en caso de cualquier eventualidad.
- Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad. Las estaciones situadas en la banda de bajas frecuencias (la banda C) están dotadas de grandes antenas (de unos 30 metros de diámetro) y son extremadamente sensibles a las interferencias. Por este motivo suelen estar situadas lejos de áreas habitadas. Las estaciones que trabajan en la banda Ku disponen de una antena menor y son menos sensibles a las interferencias. Utilizar un enlace de microondas de alta capacidad sólo ayudaría a complicar los problemas de ruido que presente el enlace con el satélite.
- Las comunicaciones con el satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación. Es necesario utilizar técnicas de encriptación para garantizar la privacidad de los datos.
- Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol en el que la tierra se sitúa entre el Sol y el satélite, se corta el suministro de energía a las células solares que alimentan el satélite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción de las potencialidades o en una pérdida de servicio.
- En el caso de tránsitos solares, el satélite pasa directamente entre el Sol y la Tierra provocando un aumento del ruido térmico en la estación terrena, y una pérdida probable de la señal enviada por el satélite.
- Actualmente hay un problema de ocupación de la órbita geoestacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados (anteriormente era de 4). Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda en forma de ruido.

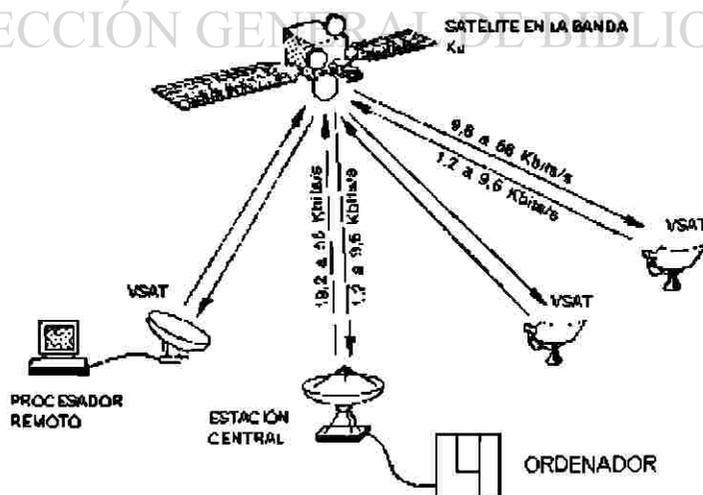


Figura: La red de datos de AT&T utiliza un satélite para conectar las estaciones a una estación central

CABLEADO ESTRUCTURADO

Es la organización de cables dentro de un edificio que recoge las necesidades de comunicación (teléfonos, ordenadores, fax, módems, etc.) actuales y futuras de las empresas. Este tipo de instalaciones hay que tenerlas en cuenta del mismo modo que se hace con la electricidad, agua, gas, etc.

Un sistema de cableado está determinado por el tipo de cable y la topología del sistema. Mientras que el tipo de cable decide la manera de realizar el sistema, la topología decide los costos de la instalación, los costos de la futura expansión, así como en algunos casos la complejidad de modificaciones dentro de la red.

A la hora de realizar el cableado de un edificio hay que tener en cuenta que la tecnología varía a tal velocidad que las nuevas tendencias pueden hacer quedar obsoleta cualquier solución adoptada que no prevea una gran capacidad de adaptabilidad.

Por este motivo aparece el concepto de “cableado estructurado”. Su intención es:

- Capacidad de crecimiento a bajo costo.
- Base para soportar todas las tecnologías de niveles superiores sin necesidad de diferentes tipos de cableado
- Realizar una instalación compatible con las tecnologías actuales y las que estén por llegar.
- Tener la suficiente flexibilidad para realizar los movimientos internos de personas y máquinas dentro de la instalación.
- Estar diseñado e instalado de tal manera que permita una fácil supervisión, mantenimiento y administración. Deberá ser fácilmente gestionable y muy confiable.

En definitiva, todas son razones básicamente económicas.

DIRECCIÓN GENERAL DE BIBLIOTECAS

TOPOLOGÍAS EN EL CABLEADO ESTRUCTURADO

El cableado estructurado reduce todas las topologías a una sola, **la estrella**. Todos los puestos se unirán a través de los elementos de interconexión física a un único punto. Esto puede ser así porque cualquier topología se puede convertir en una estrella.

El cableado estructurado consiste por tanto en fijar una disposición física del cable tirado en una instalación, de tal modo que se optimicen al máximo las posibilidades de una red y nos permita una gran facilidad de manejo y migración a nuevas tecnologías y situación física de los usuarios y servidores.

ESTÁNDARES

Dada la gran variedad de fabricantes y filosofías, para conseguir que el cableado sirva para todas ellas y las que estén por venir, es necesario que exista una normativa en cuanto a lo que va a correr por la red, cómo lo va a hacer y lo que precisa para que esto ocurra. Es vital fijar los parámetros, que deben ser comunes para todos, de tal manera que la forma en la que esté realizada la infraestructura no fije un modo de funcionamiento para cada una de ellas, y además, es preciso que todos los dispositivos (actuales y en desarrollo) se adapten a estas normas.

Existen una serie de organizaciones y comités internacionales que se encargan de fijar una serie de "reglas generales para todos". (ANSI, CCITT, EIA/TIA).

NORMATIVAS PARA EL CABLEADO ESTRUCTURADO

El Sistema de Cableado constituye el nivel de infraestructura básica de una red de comunicaciones, su buen diseño y correcta instalación son de suma importancia teniendo en cuenta que es una de las principales causas que pueden afectar al buen funcionamiento de una red. Por otra parte, siempre hay que tener presente los estándares que marcan la calidad en un Sistema de Cableado, utilizando material de fabricantes reconocidos y las instalaciones se deben llevar a cabo siguiendo las normativas más adecuadas en cada caso

Un sistema de cableado estructurado tiene (en su parte física) dos partes fundamentales, y en este sentido están fijados por las normas.

- Por un lado tenemos el cable en sí mismo, y las normas exigen para cada cable y para cada modo de funcionamiento unas determinadas formas de comportamiento, fundamentalmente relacionadas con la velocidad de transmisión, la longitud del cable y la atenuación que se produce en la señal.
- Por otra parte tenemos el modo de conexión del cable, fijándose una serie de recomendaciones en el sentido de hacer lo más común para todas las instalaciones la manera de conectar los distintos subsistemas que forman parte de la red.

CABLES: TIPOS DE CABLES EN EL CABLEADO ESTRUCTURADO

Aunque existen muchos tipos de cables, al estandarizar las instalaciones se ha limitado, por sentido común, la utilización de dos tipos de cables: el Par Trenzado en cobre y la Fibra Óptica. Una masiva utilización de estos cables ha permitido que los precios de fabricación bajen. La menor utilización del cable coaxial se debe a su mayor costo, menor flexibilidad en cuanto a sus posibilidades de uso y un mayor tamaño que complica su tendido y aumenta la ocupación de los conductos.

La importancia de los cables es fundamental en la construcción de la red, pues determinan el límite de velocidad de ésta.

PROTOCOLO TCP/IP

Se trata de un conjunto de protocolos, aunque los más conocidos sean TCP (nivel de transporte) e IP (nivel de red). Las aplicaciones que corren sobre TCP/IP no tienen que conocer las características físicas de la red en la que se encuentran; con esto, se evita el tener que modificarlas o reconstruirlas para cada tipo de red. Esta familia de protocolos genera un modelo llamado INTERNET, del cual en general tenemos un amplio conocimiento.

CARACTERÍSTICAS DE TCP/IP

Las principales características son:

- Utiliza conmutación de paquetes.
- Proporciona una conexión confiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
- Se apoya en los protocolos de más bajo nivel para acceder a la red física (Ethernet, Token-Ring).

FUNCIONAMIENTO DE TCP/IP

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes conteniendo :

- La información a transmitir.
- La dirección IP del destinatario.
- La dirección IP del remitente.
- Otros datos de control.

PROTOCOLO IP

Se trata de un protocolo a nivel de red cuyas principales características son:

- Ofrece un servicio no orientado a la conexión; esto significa que cada trama en la que ha sido dividido un paquete es tratado por independiente. Las tramas que

componen un paquete pueden ser enviadas por caminos distintos e incluso llegar desordenadas.

- Ofrece un servicio no muy confiable porque a veces los paquetes se pierden, duplican o estropean y este nivel no informa de ello pues no es consciente del problema.

DIRECCIONAMIENTO IP

Cada máquina con TCP/IP tiene asociado un número de 32 bits al que se llama dirección IP, y que está dividido en dos partes:

- **Una parte que identifica la dirección de la red (NET ID).** Esta parte es asignada por el NIC (Network Information Center). Si la red local no va a conectarse con otras redes, no es necesario solicitar a ese organismo una dirección. El número de bits que ocupa esta parte depende del tamaño de la red y puede ser 8, 16 ó 24.
- **Una parte que identifica la dirección de la máquina dentro de la red (HOST ID).** Las direcciones de los hosts son asignadas por el administrador de la red.

Una dirección se representa por cuatro valores decimales separados por puntos, para que sea más fácil su escritura y memorización.

[0..255] . [0..255] . [0..255] . [0..255]

MÁSCARA DE SUBRED

Cuando una red aparece segmentada (dividida en subredes), se debe utilizar un dispositivo que interconecte los segmentos y se hace necesario identificar de algún modo cada uno de los segmentos. Si todos los segmentos tienen la misma dirección IP, se hace necesaria la existencia de algún mecanismo que diferencia los segmentos. Este mecanismo es la máscara de la subred.

A cada dirección IP de red, es decir, a cada red física, se le asocia una máscara que tiene 32 bits. La máscara sirve para dividir la parte de la dirección IP destinada a identificar el host en dos partes: la primera identificará el segmento, y la segunda el host dentro de este segmento. En esta máscara los bits a 1 significan que el bit correspondiente de la dirección IP será tratado como bit correspondiente a la dirección de la subred, mientras que los bits a 0 en la máscara, indican que los bits correspondientes de la dirección IP serán interpretados como identificadores del host. Así con una misma dirección de red se pueden direccionar muchas subredes.

DIRECCIONES UTILIZADAS

Cuando se intenta establecer una conexión con otra máquina, no se suele poner la dirección IP de esta, sin que se utiliza un nombre. La máquina se encarga de transformar ese nombre a una dirección IP.

Cuando se quiere conectar con otra máquina que no está en la misma red, se suele utilizar un nombre que es más complejo que las conexiones dentro de la misma red. Dicho nombre consta de dos partes:

- Identificación del usuario@.
- Nombre de la máquina.

El nombre de la máquina se llama dominio, que a su vez puede estar dividido en subdominios. Lo normal es que un dominio tenga tres subdominios, de los cuales el de más a la derecha se denomina subdominio de primer nivel y es el más genérico de todos.

Para entender los subdominios se deben mirar de derecha a izquierda. Existen dos tipos de subdominios de primer nivel:

Domínios de organizaciones, utilizados casi de manera exclusiva en Norteamérica.

Domínios geográficos utilizados en el resto del mundo.

Subdominio 1º nivel. Organizaciones	Significado
Com	Organización comercial
Edu	Educativa
Gov	Gobierno
int	Organización internacional
Mil	Organización militar
Net	Gestión de redes
Org	Organización no lucrativa

Subdominio 1º nivel. Geográficos	Significado
At	Austria
Au	Australia
Ca	Canadá
de	Alemania
Mx	México
Fr	Francia
Uk	Reino Unido

El siguiente dominio suele hacer referencia a la institución en concreto, no al tipo, a través de las iniciales de esta.

El último dominio hace referencia al nombre de la máquina.

Ejemplos de direcciones

agonzalez@yahoo.com

esanchez@hotmail.com

uarteaga@terra.com.mx

rperez@enlace.net

ogomez@ctrvax.vanderbilt.edu

Se suelen utilizar siempre letras minúsculas para los nombres asociados a las direcciones IP

RELACION ENTRE DIRECCIONES IP Y DIRECCIONES FÍSICAS

Se debe relacionar la dirección IP suministrada con una dirección física. Situándose en la jerarquía de niveles utilizada por Internet, se observa que por debajo del protocolo IP existe el nivel de enlace, en el se asientan protocolos como ARP o RARP. Estos protocolos resuelven problemas relacionados con las direcciones.

ARP: Convierte una dirección IP en una dirección física.

RARP: Convierte una dirección física en una dirección IP.

En cada host debe existir una tabla de encaminamiento, que está limitada a la red que pertenece. Si la dirección IP no pertenece a la red, entonces hace dirigir los paquetes IP hacia el gateway o router que esté conectado a esa red, el cual ya poseen unas tablas que referencias las redes que conocen. El contenido de estas tablas puede variar dinámicamente.

PROTOCOLO TCP

Sus principales características son:

- Se trata de un protocolo orientado a la conexión.
- Orientado al flujo: el servicio TCP envía al receptor los datos en el mismo orden en que fueron enviados.
- Conexión con circuito virtual: no existe conexión física dedicada; sin embargo, el protocolo hace creer al programa de aplicación que sí existe esta conexión dedicada.

SISTEMAS OPERATIVOS DE RED

Los sistemas operativos de red, además de incorporar herramientas propias de un sistema operativo como son por ejemplo las herramientas para manejo de archivos y directorios, incluyen otras para el uso, gestión y mantenimiento de la red, así como herramientas

destinadas a correo electrónico, envío de mensajes, copia de archivos entre nodos, ejecución de aplicaciones contenidas en otras máquinas, compartición de recursos hardware etc. Existen muchos sistemas operativos capaces de gestionar una red dependiente de las arquitecturas de las máquinas que se utilicen. Los más comunes son : Novell, Lantastic, Windows 3.11 para trabajo en grupo, Unix, Linux, Windows 95, Windows NT, OS/2, etc. Cada sistema operativo ofrece una forma diferente de manejar la red y utiliza diferentes protocolos para la comunicación.

ACCESO REMOTO A LA RED LOCAL

Las redes locales actuales pueden extenderse más allá de los límites del propio lugar de trabajo. Con la informática móvil y la proliferación de las redes locales, es necesario que cuando un usuario se encuentre fuera de su lugar de trabajo exista alguna posibilidad de conectar con la red local de la empresa, ya sea para consultar correo electrónico, para enviar datos o imprimir un informe en un dispositivo de la propia empresa para que lo puedan ver otras personas de la compañía.

El acceso remoto a redes ofrece una función principal: permite acceder a los recursos de la red de la compañía, luego se permite acceder a archivos que se encuentran en el servidor de red de la empresa, y se garantiza que todos los usuarios puedan acceder a una misma copia de un archivo, de forma que cualquier modificación realizada por un usuario queda disponible para todos los demás que tengan permisos para consultarlo.

Si la red local de la compañía posee acceso permanente a la red, los usuarios que se conectan de forma remota pueden utilizar dicho recurso. De este modo, la empresa se convierte en un proveedor de Internet que proporciona acceso a sus propios empleados.

Todo este acceso lo facilita la red telefónica tanto la fija como la móvil (Celular). El aspecto de la telefonía móvil resulta muy interesante, ya que en la actualidad un teléfono Celular se puede conectar a una computadora (normalmente un portátil). El problema es el elevado precio de las llamadas, aunque no lo es tanto. Si se observan las tarifas de llamadas telefónicas móviles a teléfonos fijos en un horario determinado por cada compañía telefónica (que suelen denominar *reducido*), veremos que son inferiores a las llamadas nacionales, por lo que una llamada desde Monterrey a Guadalajara por celular puede resultar más barata que el teléfono fijo. Pero generalmente el horario reducido no coincide con las necesidades de comunicación de los usuarios y se hace necesario disponer de otra fuente de comunicación más barata. Por ello, si la red local tiene acceso a Internet, mediante un servicio que proporciona la compañía Telefónica que nos dé servicio podemos conectar con la red de la empresa al precio de una llamada local.

INTRANET

Una intranet no es más que una red local funcionando como lo hace Internet, es decir usando el conjunto de protocolos TCP/IP en sus respectivos niveles. Este concepto es reciente y engloba a todo un conjunto de redes locales con distintas topologías y cableados, pero que en sus niveles de transporte y de red funcionan con los mismos protocolos.

Este hecho, facilita enormemente la conexión con otros tipos de redes a través de Internet, puesto que utiliza sus mismos protocolos. Además todas las herramientas y utilidades que existen para Internet, se pueden utilizar en una intranet (creación de páginas Web, correo electrónico, IRC, etc.

SOFTWARE DE INTRANETS

CORTAFUEGOS (FIREWALL)

Una intranet puede estar conectada al mundo exterior (Internet) o no. Si lo está, se debe tener cuidado en su seguridad, ya que si no existe ninguna limitación de accesos, cualquier *figón* podría entrar en la red y jugar con las bases de datos o con los archivos. Para evitar estos problemas, se utilizan los cortafuegos, que son programas que pueden impedir que visitantes no autorizados accedan a recursos sensibles de una intranet, al tiempo que permiten el acceso a recursos públicos como el servidor Web corporativo.

Uno de los beneficios del cortafuegos, es que oculta los datos sobre la sede y la intranet a las miradas curiosas: cuanta menos gente de fuera sepa de la existencia de la red, más difícil será sabotearla.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

GROUPWARE

No es nada fácil proporcionar una definición breve y precisa de lo que es *Trabajo en Grupo* o *GroupWare*. Lo que sí parece claro, es que todos los interesados están de acuerdo en que la gran función que tiene a su favor es el aprovechamiento máximo que se obtiene tanto de los conocimientos de sus empleados, comerciales y demás personas involucradas, como de su experiencia.

El motivo de que no exista ninguna definición clara y detallada de *Trabajo en Grupo* es debido a que en dicho concepto convergen elementos tecnológicos que hasta hoy en día eran totalmente independientes: mensajería electrónica, bases de datos compartidas, herramientas de automatización del flujo de trabajo, etc., de hecho cada uno de estos elementos por separado, bien podrían valer para definir el *Trabajo en Grupo*, el problema está en que dependiendo de las prioridades de cada individuo, una definición se adaptará más que otra a sus propósitos: la tecnología de comunicaciones verá en la mensajería electrónica su base principal y los distribuidores de aplicaciones de trabajo compartido,

considerarán las bases de datos y la conferencia electrónica como piedra angular de esta nueva categoría de aplicación informática.

La característica más destacada de las aplicaciones de *Trabajo en Grupo* es que permiten a las personas trabajar juntas de forma más rápida, eficaz y productiva. Según esto y con lo ya visto, podemos plantear este nuevo concepto como una interacción dinámica entre tres importantes elementos:

- La **comunicación** basada en potentes herramientas de mensajería electrónica
- La **colaboración** que permite el intercambio y uso compartido de información y recursos.
- La **coordinación** que relaciona los dos anteriores elementos de manera eficaz.

Esta nueva plataforma de integración debe abarcar todas las necesidades presentes y futuras que se puedan plantear en un trabajo desarrollado en grupo, esto es:

- **Integración de recursos externos:** acceso de datos desde sistemas de gestión relacional de bases de datos, aplicaciones, etc.
- **No vinculación a una sola plataforma:** aunque las aplicaciones de *Trabajo en Grupo* suelen implementarse inicialmente a nivel departamental, muchas de ellas terminan desplegándose por toda la empresa.
- **Movilidad:** deben de existir conexiones entre redes distantes, así como con portátiles o computadoras remotas.
- **Aplicaciones inter-empresariales:** que dispongan de una serie de aplicaciones de fácil ampliación y de instalación transparente, según las necesidades.
- **Ámbito de implantación global:** que ofrezca soporte para todos los sistemas operativos de red, servidores y clientes.

Las principales características del *GroupWare* son:

- **Formatos dispares/multimedia.** Estas aplicaciones constituyen un verdadero almacén de objetos, un *contenedor* cuya estructura resulta idónea para el eficaz almacenamiento, distribución y gestión de la información utilizada a diario en cualquier empresa.
- **Búsqueda de texto en índice.** Cuentan con un potente dispositivo de búsqueda de texto en índice que agiliza la indexación y localización de documentos en función de las consultas formuladas por el usuario.
- **Control de versiones.** Las aplicaciones de *GroupWare* ofrecen una completa herramienta que permite crear distintas versiones de un mismo documento. Además, facilita el seguimiento de las distintas modificaciones realizadas sobre el documento original, por varios usuarios distintos. Los cambios incorporados por un usuario no quedan invalidados cuando otra persona almacena los suyos posteriormente. Los usuarios también pueden incorporar a un documento original comentarios y sugerencias en forma de respuesta a éste sin necesidad de volver a almacenarlo.

Como ejemplos de software que se encuentran dentro de la categoría del Groupware podemos citar los siguientes:

- Lotus Notes
- Group Wise
- Net Meeting
- Net Support School
- Web Turbo
- Comuniqué by Cipher Systems

CONCLUSIONES

Como es factible apreciar, la importancia que han cobrado las redes para la optimización del trabajo en el ámbito de las computadoras en los últimos tiempos resulta evidente. A la fecha resulta muy difícil encontrar algún trabajo que no se encuentre directa o indirectamente relacionado o soportado por este tipo de herramientas.

Las redes, nos permiten el acceso a varias funciones que se antojan demasiado complicadas o ineficientes en el caso de computadoras aisladas, tales como la compartición de archivos, impresión en impresoras físicamente dispersas, comunicación entre varios usuarios, etc.; de hecho es una verdad actual que una computadora se considera subutilizada en el caso de no encontrarse conectada o al menos contar con los medios necesarios para conectarse a una red.

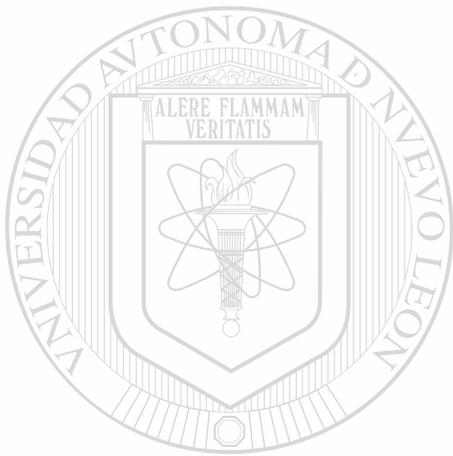
Es parte del objeto del presente documento dejar de manifiesto que la existencia de una red local dentro de una entidad productiva se ha convertido en una herramienta poderosa para el ejercicio de sus actividades cotidianas y especiales. Ya que estas nos brindan un medio efectivo para el manejo y distribución de la información que se genera con motivo de sus operaciones.

Resulta ineludible el remarcar que como resultado de las necesidades en particular de cada organización debe tomarse la decisión de que tipo de red resulta la más conveniente implementar, es decir, que no debemos sujetarnos a las "modas" impuestas por el mercado tecnológico, sino al resultado de un análisis minucioso de cómo opera cada entidad, los requerimientos que dicha operación genera y los recursos con los que se cuentan. Además, otro factor que resulta fundamental es el tener en cuenta y lo más claro que sea posible, las facilidades de crecimiento y escalabilidad de la red local que se pretende implementar, ya que esto nos evitará en un futuro dolores de cabeza y costos elevados cuando pretendamos extender la cobertura de la red a nuevos usuarios.

También forma parte del objetivo del presente escrito, el contar con un documento de ágil consulta e introducción académica, más que técnica, en cuestiones relacionadas a redes locales, pretendiendo arrojar un poco de luz a este ámbito que en ocasiones nos resulta un

poco obscuro cuando pretendemos entender la manera en que estos, a veces complicados sistemas de manejo de información operan.

Por último, resulta conveniente manifestar que a mi juicio y en virtud de que la tendencia de cualquier organización se dirige hacia el incremento de sus volúmenes de información, me conduce a visualizar que en un futuro a corto plazo, serán requeridos sistemas de redes locales con un robustecimiento tanto en su capacidad de procesamiento, almacenamiento y en las facilidades que brinden las aplicaciones y sistemas operativos que se manejen o pretendan manejar en estas, ya que factores como la competencia y el servicio a sus clientes demandarán un medio más eficiente para el manejo de la información.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

GLOSARIO DE TÉRMINOS

Presento a continuación un glosario de términos que no pretende ser un diccionario. En vez de darle una estructura alfabética, he preferido una organización a nivel de conocimientos; así el lector encontrará en su lectura lineal, la explicación a muchos de los términos que aparecen en este texto.

Cliente: cualquier estación de trabajo de una red que solicita servicios a un servidor de cualquier naturaleza.

Estación de trabajo: cualquier ordenador conectado a la red. Antiguamente sólo se llamaba estación de trabajo a los ordenadores más potentes, en la actualidad no es así. Evidentemente todas las estaciones de trabajo deben incorporar su tarjeta de red; esto no impide que la estación pueda trabajar de forma independiente y utilizar los servicios de la red cuando le sea necesario.

Nodo: cualquier estación de trabajo, terminal, computadora personal, impresora o cualquier otro dispositivo conectado a la red. Por lo tanto, este término engloba al anterior. Los dispositivos pueden conectarse a la red a través de una computadora, o bien directamente si éstos son capaces de soportar una tarjeta de red.

Servidor: se trata de una estación de trabajo que gestiona algún tipo de dispositivo de la red, como pueden ser impresoras, faxes, modems, discos duros, etc., dando servicio al resto de las estaciones, no siendo necesario que dichos dispositivos estén conectados de forma directa a esta estación. Por tanto, se puede hablar de servidor de impresión, servidor de comunicaciones, servidor de archivos, etc. Estos servidores pueden ser dedicados, cuando no pueden utilizarse para otra cosa, o no dedicados, cuando funcionan como una computadora más de la red, además de prestar servicios como servidor de algún elemento.

Medio de transmisión: se trata de cualquier medio físico, incluso el aire (como por ejemplo en las comunicaciones inalámbricas o por radio), que pueda transportar información en forma de señales electromagnéticas. El medio de transmisión es el soporte de toda la red: si no tenemos medio de transmisión, no tenemos red. Existen diferentes medios de transmisión: cable coaxial, fibra óptica, par trenzado, microondas, ondas de radio, infrarrojos, láser, etc. La elección del medio de transmisión para una red no se hace de forma aleatoria; existen un serie de factores que lo determinan: la velocidad que queramos en la red, la arquitectura, el ruido e interferencias que va a tener que soportar, la distancia, etc.

Método de acceso al medio: una vez que se tiene seleccionado el medio de transmisión que se va a utilizar para implementar la red, se debe elegir el método que los diferentes nodos de la red van a emplear para acceder a dicho medio. En un principio se podría obviar esta cuestión, pero si el lector se detiene un momento a pensar en el siguiente ejemplo, se

dará cuenta de la necesidad de esta política. El ejemplo es el siguiente: Imagine, que tiene dos computadoras que quieren utilizar la red para enviar información en un instante determinado. Si los dos ordenadores colocan en el medio físico, sin más, la información, puede ser que ambos paquetes de información “choquen” y se deterioren, no llegando ninguno de ellos a su destino. Obviamente, cuando varios dispositivos están compartiendo un medio común, es necesaria la implantación de una política de uso de dicho medio: se trata de un método de acceso al medio. Se podrían citar como medios más comunes el paso de testigo, acceso múltiple por detección de portadora con y sin detección de colisiones, polling, contención simple, etc. En cada topología de red se utiliza el más conveniente de estos métodos; por ejemplo, cuando se tiene una red en anillo, el método de acceso al medio utilizado es el paso de testigo, mientras que si tenemos una topología en bus, los métodos de contención son lo más adecuados. Los métodos de control de acceso al medio se encuentran dentro del nivel de enlace de la torre OSI, por lo que en realidad pueden entenderse como protocolos de red.

Protocolos de red: ya se ha establecido cómo van a acceder los diferentes nodos a la red y ahora es necesario especificar cómo van a comunicarse entre sí. Los protocolos de red definen las diferentes reglas y normas que rigen el intercambio de información entre nodos de la red. Los protocolos establecen reglas a muchos niveles: desde cómo acceder al medio, hasta cómo encaminar información desde origen hasta su destino, pasando por la descripción de las normas de funcionamiento de todos y cada uno de los niveles del modelo OSI de la ISO. Por citar algunos ejemplos de protocolos, nombraremos varios: TCP (protocolo de control de transmisión), IP (protocolo Internet), FTP (protocolo para transferencia de ficheros), X.25, etc.

ISO (International Organization for Standardization): Se trata de una organización reconocida mundialmente de normalización. Su objetivo es el de promover y desarrollar normas para el intercambio internacional. Establece normas de estandarización en muchos campos, estableciendo modelos a seguir para todos y cada uno de ellos. Abarca campos tan dispares como el diámetro de algunos tipos de conectores, el paso de rosca de tornillos, el grosor de un modelo concreto de cable, etc. En cuanto al campo de las comunicaciones, la ISO ha desarrollado un modelo, al que llamó OSI. Sus normas fomentan los entornos abiertos de conexión de red, que permiten a sistemas de diferentes casas comerciales comunicarse entre sí mediante el uso de protocolos.

OSI (Open System Interconnection): se trata de un modelo elaborado por la ISO que define los protocolos de comunicación en siete niveles diferentes. Estos niveles son los siguientes: aplicación, presentación, sesión, transporte, red, enlace y físico. Cada nivel se encarga de una parte en el proceso de transmisión (en el proceso de elaboración de la información a transmitir), apoyándose en los servicios que le ofrece el nivel inferior y dando servicios a niveles superiores.

Cada nivel tiene funciones muy definidas, que se interrelacionan con las funciones de niveles contiguos. Los niveles inferiores definen el medio físico, conectores y componentes que proporcionan comunicaciones de red, mientras que los niveles superiores definen cómo acceden las aplicaciones a los servicios de comunicación.

Paquete: un paquete es básicamente el conjunto de información a transmitir entre dos nodos. Cuando una aplicación quiera enviar información a otra aplicación de otro nodo, lo que hace es empaquetar dicha información, añadiendo datos de control como la dirección de la máquina que envía la información (dirección origen) y la dirección de la máquina a la que va destinada la información (dirección destino). Por tanto, cuando se habla de empaquetamiento, se hace referencia al proceso de guardar dentro de un paquete la información que se quiere transmitir.

Dirección: todos los nodos de la red deben tener una dirección que los identifique dentro de esta, de forma única, al igual que todos tenemos una dirección postal para poder recibir correo. La dirección de un nodo depende del protocolo IP (de la familia de protocolos TCP/IP) y en general codifican la red (recordamos que podemos interconectar distintas redes) y también codifican el nodo dentro de la red. El número asignado a cada una de estas partes depende del tipo de red que tengamos.

Ahora ya estamos en condiciones de entender cosas como “direccionamiento IP” (no es más que enviar un paquete a otro nodo utilizando para ello direcciones con el formato que el protocolo IP impone).

TCP/IP: se ha puesto muy de moda hablar de TCP/IP, ¿pero qué es TCP/IP? TCP/IP son dos protocolos de comunicaciones: el protocolo TCP (Protocolo de control de transmisión) que se establece a nivel de transporte del modelo OSI y el protocolo IP (Internet Protocol), que pertenece al nivel de red. En realidad, cuando se utiliza el término TCP/IP se hace referencia a una familia muy amplia de protocolos representada por ambos. Estos protocolos son lo que utiliza Internet para la interconexión de nodos. Sobre ellos se establecen otros protocolos a niveles superiores hasta llegar al nivel de aplicación (el más cercano al usuario), en el que se encuentran protocolos tan conocidos como FTP (Protocolo para transferencia de archivos) y que todo aquel que se haya conectado vía TCP/IP a otro nodo habrá utilizado para poder traerse archivos.

Interconexión de Redes: a veces se plantea la necesidad de interconectar dos o más redes, por ejemplo por necesidades de compartir recursos; y otras veces se necesita la división en dos subredes de una red para mejorar el rendimiento de ésta, por ejemplo. En ambos casos es necesaria la presencia de un dispositivo, que puede ser un hub, un bridge, un router, etc. Cada uno de estos dispositivos está diseñado para interconectar redes; la diferencia estriba en el nivel en el que es necesario interconectarlas: no es lo mismo interconectar dos redes con la misma arquitectura que dos redes de arquitecturas diferentes y con diferentes protocolos.

Hubs (concentradores): dispositivo que centraliza la conexión de los cables procedentes de la estaciones de trabajo. Existen dos tipos de concentradores: pasivos y activos. Los concentradores pasivos son simplemente cajas que disponen de unos puertos a los que se conectan las estaciones de trabajo dentro de una configuración en forma de estrella. Únicamente se trata de una caja de uniones.

Un concentrador activo es un concentrador que dispone de más puertos que uno pasivo para la conexión de estaciones y que realiza más tareas, como puede ser la de amplificación de la señal recibida antes de su retransmisión. A veces se utilizan para estructurar la topología de una red, permitiendo mayor flexibilidad en la modificación de ésta.

Bridges (puentes): nos permiten dos cosas: primero, conectar dos o más redes entre sí, aun teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red, y segundo, segmentar una red en otras menores. Los puentes trabajan en el nivel de enlace del modelo OSI de la ISO. Algunos de los motivos que nos pueden inducir a instalar un puente son ampliar la extensión de una red y/o el número de nodos que la componen; reducir el cuello de botella del tráfico causado por un número excesivo de nodos unidos o unir redes de topologías similares como bus y anillo. Los puentes se pueden crear incorporando dos tarjetas de red (una de cada una de las redes a interconectar) dentro del mismo servidor (conectado obviamente a ambas redes), siempre que el sistema operativo de red de dicho servidor sea capaz de gestionarlo. Existe dos tipos de puentes: locales y remotos. Los puentes locales sirven para segmentar una red y para interconectar redes que se encuentren en un espacio físico pequeño, mientras que los puentes remotos sirven para interconectar redes lejanas.

Routers (encaminadores): se trata de dispositivos que interconectan redes a nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico y encaminamiento de paquetes por el camino más eficiente en cada momento. La diferencia fundamental con los bridges es que éstos no son capaces de realizar tareas de encaminamiento en tiempo real, es decir, una vez tienen asignado un camino entre un nodo origen y uno destino siempre lo utilizan, aunque esté saturado de tráfico, mientras que los routers son capaces de modificar el camino establecido entre dos nodos dependiendo del tráfico de la red y otros factores.

Gateways (pasarelas): se trata de computadoras que trabajan a nivel de aplicación del modelo OSI de la ISO. Es el más potente de todos los dispositivos de interconexión de redes. Nos permiten interconectar redes de diferentes arquitecturas; es decir, de diferentes topologías y protocolos; no sólo realiza funciones de encaminamiento como los routers, sino que también realiza conversiones de protocolos, modificando el empaquetado de la información para adaptarla a cada red que interconecta.

146100

