

PROTOCOLOS DE

COMUNICACIONES.

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

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

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

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

Los **protocolos** de comunicaciones definen las normas que posibilitan que se establezca una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre sí. Un **interfaz**, sin embargo, es el encargado de la conexión física entre los equipos, definiendo las normas para las características eléctricas y mecánicas de la conexión.

Todos los protocolos y estándares que se consolidan como propios de Internet han de ser organizados y dirigidos de alguna manera. Esta es la misión principal del IETF (Internet Engineering Task Force), que es una gran comunidad de carácter abierto formada por diseñadores de redes, operadores, usuarios, etc. Todos los protocolos agrupados normalmente bajo el nombre TCP/IP son estándares de Internet cuyo desarrollo depende del IETF. Las actividades que realiza el IETF se dividen en distintos grupos, llamados Working Groups (WG) con finalidades específicas, los cuales se clasifican en distintas áreas comunes (Aplicaciones, seguridad, estandarización, servicios de transporte, etc.). El IESG (Internet Engineering Steering Group) se encarga de coordinar y dirigir al IETF por medio de los directores de área, que controlan las actividades número de los Working Groups que se encuentren dentro de cada área.

Las tareas de coordinación de los números asignados a los distintos protocolos de Internet están a cargo de IANA (Internet Assigned Numbers Authority). Los protocolos definidos por el IETF y su grupo de dirección correspondiente IESG contienen ciertos valores tales como: direcciones de Internet, números de protocolos y de puertos, nombres por dominio, etc. La funcionalidad de IANA está en que todos estos parámetros deben ser únicos, y por tanto, debe existir un registro que controle los valores que se encuentran asignados.

Otra de las organizaciones de gran importancia para la comunidad de Internet es la Internet Society (ISOC). Esta es una organización no gubernamental y sin intereses económicos formada por miles de profesionales centrados en las soluciones y el progreso de Internet.

Para que un protocolo de Internet se convierta en un estándar debe pasar por una serie de estados o niveles. El nivel de proposición de protocolo es asignado cuando un protocolo tiene posibilidades de convertirse en un

estándar en el futuro, siendo recomendables algunas pruebas y revisiones hasta que el IESG considere su avance. Después del nivel de proposición el protocolo puede pasar a considerarse como un "borrador" (draft standard).

Esto sólo ocurrirá cuando hayan transcurrido al menos 6 meses desde el nivel anterior, permitiendo de esta manera que la comunidad de Internet evalúe y considere el proceso de estandarización. Durante otros 4 meses el protocolo permanecerá en este nivel mientras se hacen pruebas y se analizan los comentarios recibidos con la posibilidad de efectuar algún cambio. Finalmente, el protocolo puede llegar a convertirse en un estándar oficial de Internet a través del IESG cuando su funcionalidad ha quedado suficientemente demostrada.

DISEÑO DE

PROTOCOLO

PASOS:

- Definición Del Servicio
- Primitivas De Soporte Y Suposiciones Del Entorno
- Reglas Del Protocolo
- Vocabulario De Mensajes
- Codificación

DESARROLLO:

- Definición Del Servicio
- Se desea realizar un protocolo de aplicación que permita transferir archivos entre un SERVIDOR hacia un CLIENTE.

Un cliente al iniciar una sesión debe especificar un nombre de archivo incluyendo la ruta. El protocolo es orientado a la conexión, esto es, un cliente debe establecer una conexión primero con el servidor el cual concederá o no el permiso para la transmisión, realizará la transmisión y al final la terminará. Un servidor solo atenderá una transferencia de archivos al tiempo, por cual si en el transcurso de una transferencia le llega una petición de transferencia esta debe ser rechazada.

• Primitivas De Soporte Y Suposiciones Del Entorno

- Este protocolo operará en una red punto a punto, en un extremo el servidor y en el otro el cliente.
- El Servidor y Cliente se apoyan en los servicios ofrecidos por un STM, los cuales son NO Orientados a la conexión, mensajes de longitud variable. El protocolo de aplicación se debe apoyar en las siguientes dos (2) primitivas:

- DATA.Request (Mensaje, Longitud), equivalente a una transmisión
- DATA.Indication (Mensaje, longitud), equivalente a una recepción.

(Mensaje = buffer de longitud variable, pero con un máximo de 1500 bytes)

(Longitud = cantidad de bytes a enviar o recibidos por la red)

- El STM realiza detección y corrección de errores, es decir al usuario siempre llegan los datos buenos.

El STM es half-duplex, es decir se puede transmitir o recibir pero no los dos al tiempo.

EL PROTOCOLO

TCP/IP

El Internet es una red de ordenadores conectados juntos a través de redes de comunicaciones. Esta red consiste en enlaces de fibra óptica, satélite, radio y las líneas telefónicas. El sistema tiene ordenadores de todos los tipos y funcionamiento todo el tipo de sistemas operativos. Todos utilizan el **TCP/IP** como lenguaje común

¿Qué es TCP/IP?

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

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

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

TCP/IP se basa en software utilizado en redes. Aunque el nombre **TCP/IP** implica que el ámbito total del producto es la combinación de dos protocolos: Protocolo de Control de Transmisión y Protocolo Internet. El término **TCP/IP** no es una entidad única que combina dos protocolos, sino un conjunto de programas de software más grande que proporciona servicios de red, como registro de entrada remota, transferencia de archivo remoto y correo electrónico, etc., siendo TCP/IP un método para transferir información de una máquina a otra. Además TCP/IP maneja los errores en la transmisión, administra el enrutamiento y entrega de los datos, así como controlar la transmisión real mediante el uso de señales de estado predeterminado.

Requisitos Del Protocolo TCP/IP

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

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

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

La Estructura de TCP/IP

El modelo de comunicaciones de OSI esta definido por siete capas a diferencia del modelo TCP que define

cuatro.

- Capa de Aplicación.
- Capa de Transporte.
- Capa de Red o de Internet.
- Capa de Enlace o capa de acceso a la red.

La relación entre las capas del sistema OSI y el TCP son:

<u>TCP/IP</u>		<u>OSI</u>		<u>Capa de Aplicación</u>
<u>Capas de Aplicación</u>				<u>Presentación</u>
Sesión				Capa de Transporte
Capa de Transporte				Capa de Red
Capa de red interceptada a la de enlace.				
Capa de Enlace				Capas de Enlace y Física

Descomposición en niveles de TCP/IP.

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

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

• Nivel de aplicación

Constituye el nivel mas alto de la torre TCP/IP. A diferencia del modelo OSI, se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet. Estos servicios están sustentados por una serie de protocolos que los proporcionan. Por ejemplo, tenemos el protocolo FTP (File Transfer Protocol), que proporciona los servicios necesarios para la transferencia de ficheros entre dos ordenadores.

Otro servicio, sin el cual no se concibe Internet, es el de correo electrónico, sustentado por el protocolo SMTP (Simple Mail Transfer Protocol).

• Nivel de transporte

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores, y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos:

- **UDP:** proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extrema a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.

- **TCP** (Transport Control Protocol): es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, pérdidas de paquete, orden en que llegan los paquetes, duplicados de paquetes...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como mas información añade el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es más importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

• Nivel de red

También recibe el nombre de nivel Internet. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesarias para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra máquina. Para implementar este nivel se utilizan los siguientes protocolos:

- **IP** (Internet Protocol): es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP, checksum)
- **ICMP** (Internet Control Message Protocol): Proporciona un mecanismo de comunicación de información de control y de errores entre máquinas intermedias por las que viajan los paquetes de datos. Estos datagramas los suelen emplear las máquinas (gateways, host,...) para informarse de condiciones especiales en la red, como la existencia de una congestión, la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.
- **IGMP** (Internet Group Management Protocol): este protocolo está íntimamente ligado a IP. Se emplea en máquinas que emplean IP multicast. El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios.

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP** (Address Resolution Protocol): cuando una máquina desea ponerse en contacto con otra conoce su dirección IP, entonces necesita un mecanismo dinámico que permite conocer su dirección física. Entonces envía una petición ARP por broadcast (o sea a todas las máquinas). El protocolo establece que solo contestará a la petición, si esta lleva su dirección IP. Por lo tanto solo contestará la máquina que corresponde a la dirección IP buscada, con un mensaje que incluya la dirección física. El software de comunicaciones debe mantener una cache con los pares IP-dirección física. De este modo la siguiente vez que hay que hacer una transmisión a esa dirección IP, ya conoceremos la dirección física.
- **RARP** (Reverse Address Resolution Protocol): a veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física, para que un servidor pueda darle su correspondencia IP.
- **BOOTP** (Bootstrap Protocol): el protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser más eficiente, enviando más información que meramente la

dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante, proporciona información adicional, facilitando la movilidad y el mantenimiento de las máquinas.

• Nivel de enlace

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las máquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

Visión General de los Componentes TCP/IP

- **TELNET.** El programa Telnet proporciona capacidad de registro de entrada remoto. Esto permite a un usuario de una máquina, registrarse en otra máquina, y actuar como si estuviera directamente frente a la segunda máquina. La conexión puede hacerse en cualquier sitio del mundo, siempre y cuando el usuario tenga permiso para registrarse en el sistema remoto.
- **FTP. Protocolo De Transferencia De Archivos.** El Protocolo de Transferencia de Archivos (File Transfer Protocol, FTP) permite que un archivo de un sistema se copie a otro sistema. No es necesario que el usuario se registre como usuario completo en la máquina a la que desea tener acceso, como en el caso de Telnet, en vez de ello se puede valer del programa FTP para lograr el acceso.
- **Protocolo Simple De Transferencia De Correo.** El Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol, SMTP) se utiliza para transferir correo electrónico. Transparente para el usuario, SMTP conecta distintas máquinas y transferir mensajes de correo, de una manera similar a como FTP transfiere archivos.
- **Kerberos.** Kerberos es un protocolo de seguridad de amplio soporte que utiliza un dispositivo especial conocido como servidor de autenticación. Este revalida contraseñas y esquemas de encriptado. Kerberos es uno de los sistemas de encriptamiento más seguros utilizados en comunicaciones.
- **Servidor De Nombre De Dominio.** El servidor de nombre de dominio (Domain Name Server, DNS) habilita un dispositivo con un nombre común para que sea convertido a una dirección especial de red. Por ejemplo, no se puede tener acceso a un sistema llamado daniel_laptop desde una red del otro lado del país, al menos que éste disponible algún método de verificación de los nombres de las máquinas locales. DNS proporciona la conversión del nombre común local a la dirección física única de la conexión de red del dispositivo.
- **Protocolo Simple De Administración De Red.** El Protocolo Simple de Administración de Red (Simple Network Management Protocol, SNMP) utiliza como mecanismo de transporte el Protocolo de Datagrama de Usuario (UDP). Emplea términos diferentes de TCP/IP, como administradores y agentes en vez de clientes y servidores. Un agente proporciona información sobre un dispositivo, en tanto que el administrador se comunica a través de la red.
- **Protocolo Trivial De Transferencia De Archivos.** El Protocolo Trivial de Transferencia de Archivo (Trivial File Transfer Protocol, TFTP) es un protocolo de transferencia de archivos muy sencillo, sin complicaciones, que carece totalmente de seguridad. Utiliza al UDP como transporte.
- **Protocolo De Control De Transmisión.** El Protocolo de Control de Transmisión (Transmission Control Protocol, TCP) es un protocolo de comunicaciones que proporciona transferencia confiable de datos. Es responsable de ensamblar datos pasados desde aplicaciones de capas superiores a paquetes estándar y asegurarse que los datos se transfieren correctamente.

- **Protocolo De Datagrama De Usuario.** El Protocolo de Datagrama de Usuario (User Datagram Protocol, UDP) es un protocolo orientado a comunicaciones sin conexión, lo que significa que no tiene mecanismo para la retransmisión de datagramas (a diferencia de TCP, que es orientado a conexión). UDP no es muy confiable, pero sí tiene fines particulares. Si las aplicaciones que utilizan UDP tienen su propia verificación de confiabilidad, los inconvenientes de UDP se pueden superar.
- **Protocolo Internet.** El Protocolo Internet (Internet Protocol, IP) es responsable de mover a través de las redes los paquetes de datos ensamblados, ya sea por TCP o UDP. A fin de determinar enrutamientos y destinos, utiliza un conjunto de direcciones únicas para cada dispositivo en la red.

Clases Direcciones Internet (IP)

Cada máquina en la Internet tiene una dirección única, esta dirección de 32 bits esta dividida en dos partes:

- Bits de Red.
- Bits de Host.

Estas direcciones son asignadas por un organismo central (NIC, Network Information Center).

• Dirección clase A

Las direcciones de clase A corresponden a redes que pueden direccionar hasta 16.777.214 máquinas cada una. Las direcciones de red de clase A tienen el primer bit a 0. Solo existen 124 direcciones de red de clase A.

Ejemplo:

0 Red (7 bits) Máquina (24 bits)

00001010 00001111 00010000 00001011

10 15 16 11

10.15.16.11 (Notación decimal)

Rangos:

1.xxx.xxx.xxx – 126.xxx.xxx.xxx

• Dirección clase B

Las direcciones de red de clase B permiten direccionar 65.534 máquinas cada una. Los primeros bits de una dirección de red de clase B son 0–1. Existen 16.382 direcciones de red de clase B.

Ejemplo:

01 Red (14 bits) Máquina (16 bits)

01000001 00001010 00000010 00000011

129 10 2 3

129.10.2.3 (Notación decimal)

Rangos:

128.001.xxx.xxx – 191.254.xxx.xxx

- **Dirección clase C**

Las direcciones de clase C permiten direccionar 254 máquinas. Las direcciones de clase C empiezan con los bits 110. Existen 2.097.152 direcciones de red de clase C.

Ejemplo:

110 Red (21 bits) Máquina (8 bits)

11001010 00001111 00010111 00001011

202 15 23 11

202.15.23.11 (Notación decimal)

Rangos:

192.000.001.xxx – 223.255.254..xxx

- **Dirección clase D**

Las direcciones de clase D son un grupo especial que se utiliza para dirigirse a grupos de máquinas. Estas direcciones son muy poco utilizadas. Los primeros bits de una dirección de clase D son 1–1–1–0.

1110 Dirección múltiple

Rangos:

224.000.000.000 hasta 239.255.255.254

La clase se identifica mediante las primeras secuencias de bits, y en los ejemplos se muestra como 1 bits para la clase A y hasta 4 bits para la clase D. La clase puede determinarse a partir de los 3 primeros bits (de orden más alto). De hecho, en la mayor parte de los casos basta con los dos primeros bits, ya que existen pocas redes Clase D.

HDLC

CONCEPTOS BASICOS

HDLC (High–Level Data Link Control) es un protocolo orientado a bit del nivel de enlace. **HDLC** fue especificado por la **ISO**, luego de que IBM a mediados de 1973 anunciara que en sus productos de comunicaciones trabajarán con un protocolo denominado **SDLC** (Synchronous Data Link Control), basado en un entorno centralizado (por sondeo) y estrategias de envío continuo y repetición

Nivel De Enlace.

El **Protocolo HDLC** se diseñó para proporcionar un mecanismo de detección y corrección de errores de propósito general a los enlaces digitales, entendiendo como enlace un único cable que conecta dos máquinas

(enlace punto a punto), o varias máquinas (enlace multipunto); este protocolo es muy extenso, por lo que rara vez se utiliza la implementación completa; lo normal es que se utilicen subconjuntos.

La tarea principal del nivel de enlace (nivel 2 OSI) consiste en, a partir de un medio de transmisión común y corriente, transformarlo en una línea sin errores de transmisión para la capa de red (nivel 3 OSI).

Los protocolos del nivel de enlace definen, típicamente, reglas para: iniciar y terminar un enlace (sobre un circuito físico previamente establecido), controlar la correcta transferencia de información y recuperarse de anomalías.

El **HDLC** consiste en tramas de bits que están delimitadas por unas banderas de 8 bits de longitud que contienen el valor **01111110** binario. Cuando el receptor encuentra este valor en el canal, comienza la lectura de una trama, lectura que termina cuando vuelve a encontrar este mismo valor. Nótese que una bandera puede indicar, simultáneamente, el final de una trama, y el comienzo de la siguiente. Puesto que dentro de una trama, en el campo de datos de usuario puede aparecer este valor, el transmisor insertará automáticamente un bit a 0 detrás de cada bloque de cinco bits a 1; el receptor, a su vez, eliminará cada bit a 0 que siga a un bloque de cinco bits a 1; con este esquema se garantiza que nunca aparecerá el valor de la bandera dentro de los bits de datos, es decir, el usuario puede colocar cualquier información dentro del paquete, la transmisión es totalmente transparente.

Las tramas incorporan una **dirección**, un **código de control** y unos **números de secuencia**. Los números de secuencia de recepción indican el número de secuencia de la siguiente trama que se espera recibir; así, si una trama es recibida correctamente, este valor se incrementará, haciendo que el emisor mande la siguiente trama; si la trama se pierde el valor permanecerá igual, con lo que el emisor la volverá a enviar.

Las tramas de control gestionan fundamentalmente el control de flujo y la notificación de errores.

Funciones Del Nivel De Enlace.

- Sincronización de trama y transparencia, estableciendo la delimitación de los mensajes.
- Control de errores de transmisión, introduciendo redundancia.
- Coordinación de la comunicación.
- Compartición del circuito físico entre diferentes enlaces lógicos, inclusión de direcciones.
- Recuperación ante fallos, supervisión y detección de anomalías.

Tipos De Protocolos De Control Del Enlace.

Los protocolos de control del enlace clásico han sido orientados a carácter, esto es, utilizan mensajes de control constituidos por uno o varios caracteres denominados de control que complementan los caracteres convencionales del alfabeto utilizado (EBCDIC, ASCII, etc.). Sus principales desventajas son:

- Uso de tramas multiformato: diseño complejo.
- Mensajes de control escasamente protegidos: un bit de paridad por carácter.
- Dependencia del alfabeto utilizado.

Los protocolos orientados a bit vienen a eliminar las desventajas de los anteriores. Los requisitos deseables en un protocolo del nivel de enlace se pueden resumir en:

- Independencia del alfabeto.
- Transparencia.
- Permita diversas configuraciones (dúplex/semidúplex, balanceada/no balanceada...).
- Alta eficiencia (cadencia eficaz) y fiabilidad.

- Baja sobrecarga.

Uno de los fundamentos básicos de estos protocolos es la estructura de su trama, monoformato, con un gui3n de apertura y cierre y campos de significado posicional. Entre los protocolos orientados a bit m3s utilizados podemos destacar:

- **SDLC** (Synchronous Data Link Control) Protocolo de nivel 2 de IBM. Est3a muy extendido.
- **ADCCP** (Advanced Data Communication Control Procedures) Publicado como ANSI X3.66, y salvo m3nimas variaciones es pr3cticamente id3ntico a **HDLC**.
- **LAPB** (Link Access Procedure Balanced) Protocolo de la capa de enlace de X.25.
- **LAPD** (Link Access Procedure, D Channel) Usado como control del enlace de datos en la Red Digital de Servicios Integrados (RDSI).

HDLC

CARACTERÍSTICAS BÁSICAS.

Tipos De Estaciones.

Definimos tres tipos de estaciones que dan lugar a dos configuraciones de enlace y tres modos de transferencia de datos.

- **Estaci3n primaria:** Controla las operaciones del enlace. Actúa como maestra y sus tramas son 3rdenes para las estaciones secundarias. Recibe respuestas de éstas últimas.
- **Estaci3n secundaria:** Opera bajo el control de una estaci3n primaria. Actúa como esclava de la primaria y sus tramas son respuestas. Mantiene solamente una sesi3n con la estaci3n principal y no tiene responsabilidad en el control del enlace. Las estaciones secundarias no pueden comunicarse directamente entre sí, lo hacen a trav3s de la estaci3n primaria.
- **Estaci3n combinada:** Es capaz de transmitir y recibir tanto 3rdenes como respuestas procedentes de otra estaci3n combinada.

Configuraciones Del Enlace.

- **Configuraci3n no balanceada (o no equilibrada):** para una estaci3n primaria y una o varias estaciones secundarias. Pueden ser punto a punto o multipunto, dúplex o semidúplex. Se la llama "no balanceada" porque la estaci3n primaria es responsable de controlar cada una de las estaciones secundarias y de establecer y mantener el enlace.
- **Configuraci3n balanceada (o equilibrada):** consiste en dos estaciones combinadas en un enlace punto a punto ya sea dúplex o semidúplex. Cada estaci3n tiene la misma responsabilidad en el control del enlace.

Nota: Los t3rminos balanceado y no balanceado empleados no tienen nada que ver con las característic3s el3ctric3s del circuito. De hecho el control del enlace de datos no debe ser consciente de los atributos físcos del circuito. Los dos t3rminos son usados en un contexto totalmente distinto en el nivel físcico y en el nivel de enlace.

HDLC

MODOS DE OPERACI3N.

Distinguimos tres fases en los protocolos de enlace: **Inicialización, Transferencia De Datos y Desconexión.**

Modos De Inicialización.

Existe un modo opcional de inicialización. En el mismo, una estación primaria o una combinada puede iniciar o regenerar el control del enlace con una secundaria o combinada. La forma concreta de realizarlo es dependiente del sistema y no es objeto de normalización.

Modos De Transferencia De Datos.

- Modo de respuesta normal (NRM)
 - **Configuración:** no balanceada.
 - **Tipo de enlace:** punto a punto o multipunto (máximo una estación primaria en enlaces multipunto).
 - **Transmisión:** dúplex o semidúplex (por defecto semidúplex).
 - **Observaciones:** las estaciones secundarias necesitan permiso de la primaria para transmitir por lo que la estación primaria suele utilizar técnicas de sondeo y selección.
- Modo de respuesta asíncrona (ARM)
 - **Configuración:** no balanceada.
 - **Tipo de enlace:** punto a punto o multipunto (máximo una estación primaria en enlaces multipunto).
 - **Transmisión:** dúplex o semidúplex.
 - **Observaciones:** Se permite a una estación secundaria transmitir sin recibir permiso explícitamente de la primaria; de esta forma en ARM se reduce la sobrecarga debido a que la secundaria no necesita ser sondeada para enviar datos. De todas formas la estación primaria mantiene la responsabilidad sobre tareas como recuperación ante errores, inicialización y desconexión del enlace.
- Modo de respuesta asíncrona balanceada (ABM)
 - **Configuración:** balanceada.
 - **Tipo de enlace:** punto a punto únicamente.
 - **Transmisión:** dúplex o semidúplex (por defecto dúplex).
 - **Observaciones:** utilizado principalmente en enlaces dúplex punto a punto. Requiere estaciones combinadas. Cualquiera de las estaciones puede comenzar una transmisión sin permiso de la otra y ambas tienen las mismas responsabilidades sobre el mantenimiento y control del enlace.

Modos De Desconexión.

En los modos de desconexión las estaciones están lógicamente desconectadas del enlace. Se distinguen dos modos de desconexión:

- Modo de desconexión normal (NDM). Aplicable al modo NRM. La(s) secundaria(s) no pueden hacer nada mientras no se lo indique la principal.
- Modo de desconexión asíncrona (ADM). Aplicable a los modos asíncronos (ABM y ARM). En este caso las estaciones secundarias pueden iniciar una desconexión sin que la principal se lo indique.

Nota: El término asíncrono no tiene nada que ver con el formato de los datos y el interface físico de las estaciones. Se utiliza para indicar que las estaciones no necesitan recibir una señal preliminar procedente de otra estación antes de comenzar a transmitir tráfico. Como veremos, HDLC utiliza formatos síncronos en sus tramas, esto es, se necesita sincronismo entre emisor y receptor.

HDLC

ESTRUCTURA DE LA TRAMA.

En **HDLC** se transmite de forma síncrona, esto es, se necesita la existencia de un sincronismo entre transmisor y receptor. La transmisión, tanto de datos como de control, se realiza mediante el intercambio de tramas monoformato entre dos estaciones.

El formato de la trama se ha representado en la figura y consta de los siguientes campos:

Guión.

Delimita la trama. Todas las tramas deben comenzar y terminar con este campo. El guión consiste en la secuencia binaria: 01111110 (seis "unos" limitados por "ceros").

Dentro de la trama podemos encontrar una secuencia binaria igual al guión (por ejemplo en el campo de información) lo que se interpretará en recepción como un final de trama que en realidad no es tal. Para solucionar esto y mantener la transparencia se utiliza la técnica de inserción de bit (bit stuffing). El funcionamiento es muy simple. El transmisor inserta un cero después de cualquier secuencia de cinco "unos" seguidos que vaya a enviar, excepto en el guión de principio y final de trama. En recepción se monitoriza continuamente el flujo de bits que se reciben. Cuando se recibe un "cero" seguido por cinco "unos" se mira el siguiente bit (el séptimo). Si es un "cero" el bit se deshecha pues es producto de una inserción de bit. Si es un "uno" se observa el siguiente bit (el octavo). Si es un cero se reconoce un guión. Si es un uno es que se trata de una señal de abortar o de enlace inactivo.

El enlace reconoce las siguientes secuencias de bits:

SECUENCIA DE BITS	SIGNIFICADO
01111110	Guión.
Al menos siete "unos" seguidos, pero menos de quince.	Abortar.
Quince o más "unos" seguidos.	Enlace inactivo.

Dirección.

El campo de dirección identifica la estación (secundaria o combinada) que recibe o envía la trama. Hay que hacer notar aquí las siguientes reglas:

- En las tramas de órdenes se coloca siempre la dirección de la estación destinataria.
- En las tramas de respuesta se indica la dirección de la estación remitente.

De esta forma, en el campo de dirección siempre se coloca la dirección de una estación secundaria en los modos no balanceados (NRM y ARM). Pero no hay ningún tipo de ambigüedad en dichos modos tanto en el caso punto a punto como multipunto, puesto que solamente hay una estación primaria (que transmite los órdenes y sabremos a qué estación secundaria van dirigidas) y una o varias secundarias (que transmiten las respuestas, y la primaria sabe de quién recibe la respuesta). Para el modo balanceado (recordar que ABM sólo admite enlaces punto a punto) nos permite indicar la dirección de los comandos y sus respuestas asociadas.

Existen dos modos de direccionamiento: monoocteto y multiocteto. Debe establecerse el modo de direccionamiento a utilizar antes de comenzar la transferencia de datos.

- **Monocteto:** se emplea un solo octeto podemos direccionar hasta 256 estaciones. Para tener una mayor capacidad de direccionamiento se debe usar el direccionamiento multiocteto.

- **Multiocteto:** nos va a permitir utilizar más de 256 estaciones al especificar la dirección con dos octetos o más. Se utiliza el primer bit de cada uno de los octetos para indicar si es el último octeto del campo de dirección. El octeto final debe llevar el primer bit a "uno" mientras que los octetos precedentes lo llevan a "cero".

También se permiten direcciones de grupo (multicasting) y direcciones de difusión (broadcasting). Estas últimas usadas para referirse a todas las estaciones colocando todos los bits del campo de dirección a "uno".

Información.

El campo de información contiene los datos propios de usuario. Existe solamente en las tramas I y algunas tramas U, como pueden ser las tramas UI (para transmitir información no numerada) y la trama FRMR (rechazo de trama). La longitud del campo de información es indefinida y suele ser múltiplo de 8 bits.

Secuencia De Verificación De Trama (SVT).

El campo SVT (en inglés FCS– Frame Check Sequence) se utiliza para chequear los errores de transmisión entre dos estaciones. Se aplica un código de redundancia cíclico (CRC) a los campos de dirección, control e información de la trama.

Si se emplea un CRC de 16 bits se transmite el resto de la división módulo 2 de los campos de dirección, control e información entre el polinomio.

Si se emplea un CRC de 32 bits se transmite el resto de la división módulo 2 de los campos de dirección, control e información entre el polinomio

HDLC

CAMPO DE CONTROL

El campo de control nos identifica el tipo de trama y su función concreta. El formato del campo de control se ha representado en la figura adjunta.

Como podemos ver existen tres tipos de tramas: **tramas de información (tramas I)**, **tramas de supervisión (tramas S)** y **tramas no numeradas (tramas U)**. El campo de control permite distinguir entre ellas al proporcionarnos la siguiente información:

- **N(s):** Es el número de la trama transmitida. Aparece únicamente en las tramas de información.
- **N(r):** Es el número de la trama que se espera recibir del otro extremo. Se utiliza para confirmar la recepción correcta de las tramas con $N(S) \text{ menor que } N(R)-1$.
- **S:** Dos bits para codificar los cuatro tipos existentes de tramas de supervisión.
- **M:** *Cinco bits que nos permiten definir hasta 32 órdenes y respuestas no numeradas.*

El Bit P/F.

El bit P/F (polling/final) es el quinto bit en el campo de control de las tramas HDLC. Tiene dos usos claramente diferenciados:

- **Sondeo.** *Es precisamente con la aplicación primitiva de estos protocolos cuando surge el bit P/F. Se tenían circuitos multiacceso con sondeo y modo normal de respuesta y el bit P/F se utiliza como testigo asociado al turno de transmisión. Una estación principal mantiene el bit P/F a cero mientras manda órdenes y no da opción a que las secundarias puedan responder. Cuando pone el*

bit P/F a uno (en este caso actúa el bit como sondeo –Poll) se cede el turno a la secundaria para que transmita. La secundaria emite su respuesta con el bit P/F a cero hasta que en la última trama que tiene para enviar coloca el bit P/F a uno (ahora actuará como bit F –Final) para indicar que ya no se tienen más tramas para transmitir en ese ciclo de sondeo (se devuelve el turno).

- **Sincronismo (Checkpointing – punteo).** Nos va a permitir asociar lógicamente a una trama de respuesta con la correspondiente orden que la generó. La idea es que al enviar una trama con el bit $P=1$ se inicia un temporizador y se obliga a que esa trama sea respondida cuanto antes y de forma explícita con el bit $F=1$.

Campo De Control Extendido.

El uso de tres bits para especificar $N(S)$ y $N(R)$ significa que los números de secuencia pueden oscilar entre 0 y 7. Esto implica que, como máximo, puede emplearse una ventana de transmisión de tamaño 7. Aunque puede ser suficiente para muchas aplicaciones, aquellas que estén trabajando con enlaces largos (mucho retardo) o de alta velocidad pueden requerir ventanas de transmisión mayores si se quiere una utilización eficiente del enlace. El campo de control que hemos descrito puede ser ampliado con un octeto adicional, que nos va a permitir aumentar los tres bits de numeración de secuencia de las tramas de información hasta siete bits con lo que la ventana de transmisión puede llegar hasta 127.

HDLC

TIPOS DE TRAMAS.

En HDLC se tienen tres tipos de tramas: **información, supervisión y no numeradas**; las cuales se distinguen por su campo de control.

Tramas De Información (Tramas I).

Sirven para transmitir información numerada secuencialmente. Todas las tramas de información contienen en el campo de control el número de la trama transmitida $N(S)$, y el número de la trama que se espera recibir $N(R)$ que confirma al otro extremo la recepción de todas las tramas hasta $N(R)-1$. Por tanto, en enlaces con actividad bidireccional simultánea, las tramas de información en un sentido contienen asentimientos de la comunicación en sentido opuesto (Piggybacking), lo que permite una mejor utilización del circuito de datos.

Normalmente se representan las tramas de información por la letra "I" seguida por el $N(S)$ y el $N(R)$. Así la expresión I21 quiere decir que es una trama de información con el número 2 y que se espera recibir del otro extremo la trama 1, con lo que estamos asintiendo hasta la trama cero.

Las tramas de información pueden ser tanto órdenes como respuestas (O/R).

Tramas De Supervisión (Tramas S).

Se realiza con ellas el control de flujo. También nos permiten reconocer tramas a la otra estación, puesto que incluyen el $N(R)$. Con los dos bits "S" podemos definir hasta cuatro tramas de supervisión. Las cuatro pueden utilizarse en versión de orden o respuesta, dependiendo si son generadas por una estación (o fracción de una combinada) principal o secundaria, respectivamente.

- **RR. Receptor preparado (Receive Ready).** $S=00$. Se utiliza para indicar la disponibilidad de recepción de tramas y confirmación de tramas, con el subcampo $N(R)$. Una estación primaria puede usar el comando RR para sondear a una estación secundaria colocando el bit $P=1$.
- **RNR. Receptor no preparado (Receive Not Ready).** $S=01$. Indica una indisponibilidad transitoria de recepción de tramas; realiza una función de control de flujo. También reconoce tramas anteriores

con el campo N(R). Cuando el receptor pueda aceptar tramas de nuevo enviará una trama RR.

- **REJ. Rechazo (Reject).** *S=10. Utilizado para confirmar la recepción de tramas anteriores a la N(R) y solicitar la retransmisión de la trama N(R) y posteriores.*
- **SREJ. Rechazo selectivo (Selective Reject).** *S=11. Confirma la recepción de las tramas anteriores a la N(R) y solicita la retransmisión de la N(R) exclusivamente. Una trama SREJ debe ser transmitida por cada trama errónea, pero con la siguiente limitación: solamente puede haber una trama SREJ pendiente; como el campo N(R) de la trama reconoce todas las tramas precedentes, el envío de una segunda trama SREJ contradice la primera puesto que todas las tramas I con N(S) menor que el N(R) de la segunda trama SREJ serían reconocidas.*

Existen estrategias que combinan REJ y SREJ, de forma que se envíen las menores tramas posibles. Por ejemplo, si recibimos la trama 1 bien y las siete siguientes llegan con errores, es mejor enviar un REJ2 que no un SREJ por cada una de las siete tramas erróneas.

Tramas No Numeradas (Tramas U).

Se emplean también para funciones de control como pueden ser inicialización del enlace, selección del modo de transferencia de datos, establecer variables de estado, etc. También tenemos tramas de información no numeradas, esto es, sin número de secuencia que ni se asienten ni su envío modifica el número de secuencia de las tramas numeradas.

RED DE PUNTO A PUNTO

La red punto a punto se forma mediante múltiples conexiones punto a punto entre pares de máquinas.

Para que un mensaje llegue a su destino, puede tener que pasar por uno o varios nodos intermedios. Habitualmente, existe más de un camino, cada uno con su longitud.

Por ello, los algoritmos de encaminamiento (o routing) resultan vitales. Como norma general (por supuesto con sus excepciones), las redes pequeñas que se extienden en un área geográfica limitada suelen ser redes broadcast (que es donde hay un único canal de comunicación compartido por todas las máquinas de la red), frente a las redes más extensas que suelen ser redes punto a punto.

Dentro de este tipo de redes podemos considerar dos clases. Las redes de conmutación de circuitos y las de conmutación de paquetes, también conocidas como redes de almacenamiento y reenvío (store and forward).

En las primeras, al establecer la comunicación, los canales físicos que unen ambos extremos quedan reservados para uso exclusivo hasta que la conexión se libera. En el caso de redes de reenvío, cada nodo intermedio recibe mensajes en forma de paquetes de datos y los almacena hasta que los reenvía hacia su destino final o a otro nodo intermedio.

En una red punto a punto cada máquina tiene los mismos derechos de acceso como todas las demás; no existe un local central para las aplicaciones; es decir es una colección de computadoras que comparten información igualmente, donde no existe una máquina central en la red, es decir, donde no hay un servidor dedicado y todas las Pc's de la red pueden ser Servidores o Clientes en un momento determinado

Este tipo de red tiene tres ventajas:

- Barata.
- Fácil de configurar y mantener.
- Permite compartir datos y recursos.

También presenta desventajas, como son:

- Capacidad limitada.
- No soporta más de diez usuarios.
- La administración de la red debe hacerse en cada máquina.
- Insegura.
- Difícil de conectar a plataformas y sistemas operativos distintos.
- Difícil de realizar respaldos efectivos.

En este tipo de red es necesario:

- Instalar uno o unos programas en la computadora para cargar los protocolos de comunicación. Y además que el servidor (si existe) tenga un sistema operativo de red multiusuario para poder atender a las computadoras que se conecten a él
- Cuando nos conectamos a una computadora lo que necesitamos es:
- Que la computadora a donde nos conectamos tenga la capacidad de funcionar como servidor, es decir que pueda aceptar la conexión de otro equipo, es decir, que sea un equipo multiusuario, y cada equipo que se conecta es reconocido a través de una clave y un password.

Características de la red punto a punto.

- Fundamentalmente empleada en redes de largo alcance
- Los algoritmos de routing pueden llegar a ser muy complejos. Se necesitan dos niveles de control de errores: entre nodos intermedios y entre extremos.
- La información se recibe. Una vez leído el mensaje se procesa si va dirigido a la estación, o se reenvía si tiene un destino diferente.
- Varias líneas de comunicación pueden funcionar en paralelo, por lo que pueden usarse líneas de baja velocidad (2–50 Kbps)

Los principales retardos son debidos a la retransmisión del mensaje entre varios nodos intermedios.

- El medio de transmisión incluye nodos intermedios por lo que es menos fiable.
- La redundancia es inherente siempre que el número de conexiones de cada nodo sea mayor que dos.
- Los costos de cableado son superiores, y la estación requiere al menos dos tarjetas de interfaces.

TOPOLOGÍA DE RED

La configuración de una red suele conocerse como topología de la misma. La topología es la forma (la conectividad física) de la red. El termino topología es un concepto geométrico con el que se alude al aspecto de una cosa. A la hora de establecer la topología de una red, el diseñador ha de plantearse tres objetivos principales:

- Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico (encaminamiento alternativo).
- Encaminar el tráfico entre el ETD transmisor y el receptor a través del camino más económico dentro

de la red (aunque, sí se consideran más importante otros factores, como la fiabilidad, este camino de coste mínimo puede no ser el mas conveniente).

- Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo.

Cuando hablamos de fiabilidad de una red nos estamos refiriendo a la capacidad que tiene la misma para transportar datos correctamente (sin errores) de un ETD a otro. Ello incluye también la capacidad de recuperación de errores o datos perdidos en la red, ya bien con el mantenimiento del sistema, en la que se incluyen las comprobaciones diarias; el mantenimiento preventivo, que se ocupa de relevar de sus tareas a los componentes averiados o de funcionamiento incorrecto; y en su caso, el aislamiento de los focos de avería.

El segundo objetivo a cumplir a la hora de establecer una topología para la red consiste en proporcionar a los procesos de aplicación que residen en los ETD el camino más económico posible. Para ello es preciso:

- Minimizar la longitud real del canal que une los componentes, lo cual suele implicar el encaminamiento del tráfico a través del menor número posible de componentes intermedios.
- Proporcionar el canal más económico para cada actividad concreta; por ejemplo, transmitir los datos de baja prioridad a través de un enlace de baja velocidad por línea telefónica normal, lo cual es mas barato que transmitir esos mismos datos a través de un canal vía satélite de alta velocidad.

El tercer objetivo es obtener un tiempo de respuesta mínimo y un caudal eficaz lo mas elevado posible. Para reducir al mínimo el tiempo de respuesta hay que acortar el retardo entre la transmisión y la recepción de los datos de un ETD a otro.

REDES LOCALES

Es una red de comunicación optimizada de alta velocidad, que opera en un área geográfica de tamaño reducida. Puede ser un cuarto, un edificio, un campus de menos de 5 kms y de alta velocidad. Proporciona conexión a una amplia variedad de equipos de comunicación como: Computadoras, estaciones de trabajo, scanners, faxes, unidades de cinta, unidades de disco, conexión con otras redes.

Una Red de Área Local (LAN), es una interconexión de sistemas informáticos autónomos. El usuario dispone de una maquina personal. Para ahorrar el hardware y el software se comparten los datos, los programas y algunos recursos físicos tales como impresora, scanners, plotters o servidores de archivos que son accesibles a todos a través de la red.

En general, el hecho de trabajar dentro de una red de área local, es sencillo y garantiza accesos seguros a quienes se encuentran interconectados a través de la red de alta velocidad. El usuario debe conocer los recursos de la red y su distribución; esto es para comunicarse con otro usuario, debe saber en que maquina esta, debe conocer la dirección del scanner y en que maquina están los programas que desea cargar.

Las redes de comunicación se pueden clasificar de acuerdo a su diferente cobertura en:

	En el mismo local.
LAN; Red de Área Local.	En el mismo piso.
	En el mismo edificio.
	En la misma Zona.
MAN; Red de Área Metropolitana.	En la misma Área Interurbana.
(Interconexión de LAN)	En la misma ciudad
WAN; Red de Área Amplia.	En el mismo estado.

(Interconexión de MAN).	En el mismo país.
	En el mismo continente.

Si entendemos los tipos de necesidades de comunicación a cubrir, las redes pueden ser de dos clases: Locales y Remotas.

COBERTURA DE REDES DE COMPUTADORAS.

Distancia Entre Procesadores	Ubicación En Extensión Geográfica	Nombre De La Red
10 mts.	Cuarto solo.	LAN
100 mts.	Edificio.	LAN
1000 mts.	Campus.	LAN
10 kms.	Ciudad.	MAN Enlace de LAN
100 kms.	País o Estado.	WAN Enlace de MAN
+ 100 kms.	Continente.	Interconexión de MAN

Las redes locales pueden ser Centralizadas y Distribuidas, las primeras de ellas dependen de un servidor de red central, que tienen toda la información, estando obligadas las diversas estaciones de trabajo a acceder a él para recabar información o salvarla. En el caso de las redes locales distribuidas cualquier usuario puede acceder a la información de cualquier ordenador conectado a la red. En función de cómo, donde y para que se va a utilizar una red local, podremos valorar cual se ajusta mas a nuestras necesidades.

Cuando una empresa dispone de varias Pc's y es necesario conectarlas entre sí para compartir información, la red distribuida será la solución mas rápida y con el menor coste para esa función.

TÉCNICAS DE TRANSMISIÓN

REDES DE DIFUSIÓN

Tienen un solo canal de comunicación compartido por todas las máquinas, en principio todas las máquinas podrían ver toda la información, pero hay un código que especifica a quien va dirigida.

REDES PUNTO A PUNTO

Muchas conexiones entre pares individuales de máquinas. La información puede pasar por varias máquinas intermedias antes de llegar a su destino. Se puede llegar por varios caminos, con lo que se hacen muy importantes las rutinas de enrutamiento o ruteo. Es más frecuente en redes MAN y WAN.

TOPOLOGÍA LÓGICA.

Existe una distinción entre las tipologías físicas y lógicas de red. La topología Física es la manera en que se interconectan los cables con las computadoras; es la conexión física de circuitos. La topología Lógica es el flujo de datos de una Pc a otra, la proporciona el software y es una conexión lógica. Las topologías físicas pueden ser las mismas o totalmente distintas en una red de ordenadores, como las que se mencionan a continuación:

TOPOLOGÍA HORIZONTAL

La topología horizontal o de bus es frecuente en las redes de área local. Es relativamente fácil controlar el flujo de tráfico entre los distintos ETD, ya que el bus permite que todas las estaciones reciban todas las transmisiones, es decir, una estación puede difundir la información a todas las demás. La principal limitación de una topología de bus esta en el hecho de que suele existir un solo canal de comunicaciones para todos los dispositivos de la red. En consecuencia si el canal de comunicaciones falla, toda la red deja de funcionar. Algunos fabricantes proporcionan canales completamente redundantes por si falla el canal principal, y otros ofrecen conmutadores que permiten rodear un nodo en caso de que falle. Otro inconveniente de esta configuración estriba en la dificultad de aislar las averías de los componentes individuales conectados al bus. La falta de puntos de concentración complica la resolución de este tipo de problemas.

TOPOLOGÍA JERARQUICA.

La estructura jerárquica es una de las mas extendidas en la actualidad. El software que controla la red es relativamente simple, y la topología proporciona un punto de concentración de las tareas de control y de resolución de errores. En la mayoría de los casos el ETD situado en el nivel mas elevado de la jerarquía es el que controla la red. El flujo de tráfico entre los distintos ETD arranca del ETD A. Muchos fabricantes incorporan a esta topología un cierto carácter distribuido, dotando a los ETD subordinados de un control directo sobre los ETD situados en los niveles inferiores dentro de la jerarquía, lo cual reduce la carga de trabajo del nodo central A.

Las redes con topología jerárquica se conocen también como redes verticales o en árbol. La palabra árbol alude al hecho de que su estructura parece bastante a un árbol cuyas ramas va abriéndose desde el nivel superior hasta el mas bajo.

Aunque la topología jerárquica resulta interesante por ser fácil de controlar, puede presentar ciertos problemas en cuanto a la posibilidad de aparición de cuellos de botella. En determinadas situaciones, el ETD mas elevado, normalmente un gran ordenador central, ha de controlar todo el tráfico entre los distintos ETD. Este hecho no solo puede crear saturaciones de datos, sino que además plantea serios problemas de fiabilidad, si este ETD principal falla, toda la red deja de funcionar, a no ser que exista otro ordenador de reserva capaz de hacerse cargo de todas las funciones del ETD averiado. Pese a todo, las tipologías jerárquicas se han venido usando ampliamente desde hace bastantes años, y seguirán empleándose durante mucho tiempo, ya que permiten la evolución gradual hacia una red mas compleja, puesto que la adición de nuevos ETD subordinados es relativamente sencilla.

TOPOLOGÍA EN ESTRELLA.

La topología en estrella es la mas empleada en los sistemas de comunicación de datos. Una de las principales de su empleo es histórica, la red en estrella se utilizó a lo largo de los años 60's y principios de los 70's porque resultaba fácil de controlar; su software no es complicado y su flujo de tráfico es sencillo.

Todo el tráfico emana del núcleo de la estrella, que es el nodo central, marcado como A, por lo general un ordenador posee el control total de los ETD conectados a él. La configuración de estrella es, por tanto, una estructura muy similar a la de la topología jerárquica, aunque su capacidad de procesamiento distribuido es limitado.

El nodo A es el responsable de encaminar el tráfico hacia el resto de los componentes; se encarga, además de localizar las averías. Esta tarea es relativamente sencilla en el caso de la topología de estrella, ya que es posible aislar las líneas para identificar el problema. Sin embargo y al igual que en la estructura jerárquica, una red en estrella puede sufrir saturaciones y problemas en caso de avería del nodo central. Algunas redes construidas en los años 70's experimentaron serios problemas de fiabilidad, debido a su carácter centralizado. En otros sistemas se estableció redundancia en el nodo central, como medida de seguridad, con lo cual la fiabilidad aumento considerablemente.

TOPOLOGÍA EN ANILLO.

La estructura en anillo es otra configuración bastante extendida. Como vemos en la figura 5, la topología en anillo se llama así por el aspecto circular del flujo de datos. En la mayoría de los casos, los datos fluyen en una sola dirección, y cada estación recibe la señal y la retransmite a la siguiente del anillo. La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos, tan frecuentes en los sistemas de estrella y de árbol. Además, la lógica necesaria para poner en marcha una red de este tipo es relativamente simple. Cada componente solo ha de llevar una serie de tareas muy sencillas: aceptar los datos, enviarlos al ETD conectado al anillo o retransmitirlos al próximo componente del mismo.

Sin embargo, como todas las redes, la red en anillo tiene algunos defectos. El problema mas grande es que todos los componentes del anillo están unidos por un mismo canal. Si falla el canal entre dos nodos, toda la red se interrumpe, por eso algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se produce la perdida de algún canal, otros fabricantes construyen conmutadores que dirigen los datos automáticamente, saltándose el nodo averiado, hasta el siguiente nodo del anillo, con el fin de evitar que el fallo afecte a toda la red.

TOPOLOGÍA EN MALLA.

La topología en malla se ha venido empleando en los últimos años, lo que la hace atractiva a su relativa inmunidad a los problemas de embotellamiento y averías. Gracias a la multiplicada de caminos que ofrece a través de los distintos ETD y ECD, es posible orientar el trafico por trayectorias alternativas en caso de que algún nodo este averiado u ocupado, a pesar de que la realización de este método es compleja y cara (para proporcionar estas funciones especiales, la lógica de control de los protocolos de una red en malla puede llegar a ser sumamente complicada), muchos usuarios prefieren la fiabilidad de una red en malla a otras alternativas.

Un ejemplo característico de este tipo de topología es el mismo Internet, ya que este es un enlace de terminales-servidores-mainframes ubicados sin previo estudio geográfico.

TOPOLOGÍAS HÍBRIDAS.

En la practica, rara vez se encuentra una forma pura de cualquiera de estas topologías, principalmente de bus, anillo o estrella, la mayoría de las redes son híbridas, esto es, combinaciones de estas tres topologías básicas.

TECNOLOGIA DE COMUNICACIÓN UTILIZADA EN REDES.

Las tecnologías utilizadas para la comunicación entre equipos pertenecientes a una red son las que indican la secuencia o protocolos utilizados para el transporte de la información a través del medio de transmisión utilizado. Se diferencian principalmente por la velocidad de transferencia de datos y por la configuración física de red que permiten. Las tecnologías mas comunes son Ethernet, Token Ring, FDDI y ATM, sistemas que describimos a continuación.

SISTEMA ETHERNET. Este tipo de tecnología mas utilizada en redes de área local (LAN). LA RED Ethernet apareció por primera vez en 1970 por parte de la empresa Xerox con una velocidad en ese entonces de 2.94 Mbps, velocidad muy alta para tal época. Con el paso del tiempo esta tecnología ha sufrido varios cambios, de los cuales los mas significativos son la velocidad de transferencia y la longitud máxima permitida entre los equipos.

SISTEMA TOKEN RING. La tecnología Token ring fue creada por IBM y esta destinada al uso con redes en anillo (ring) aunque realmente el alambrado es hecho en forma de estrella por medio de unas unidades especiales denominadas MSAU o unidad de acceso multiestacionario.

El Token ring viaja a través de la red por cada una de las estaciones y es el encargado de asignar los permisos para transmisión de datos. Si una estación desea transmitir información debe esperar el turno hasta que el Token ring pase por allí y la habilite para tal operación. Con este método se elimina la posibilidad de colisión ya que siempre existe una única estación que puede transmitir en determinado momento.

SISTEMA FDDI (Fiber Distributed Data Interfase). Interfase de Datos Distribuidos por Fibra, Este equipo de red utiliza la fibra óptica como principal medio de transmisión en redes de configuración en anillo, surgió gracias a la necesidad de transmisiones cada vez superiores y que sobre el mismo medio se involucran vídeo y gráficos, los cuales utilizan millones de bits en imágenes de tiempo muy cortos, sin que se genere retardos en la entrega de información a otros equipos.

La velocidad típica de transferencia de datos en las redes FDDI es de 100 Mbps. En cuanto a distancia y cantidad de terminales, una red FDDI puede contener hasta 500 estaciones con una longitud total de alcance de 60 km. aproximadamente.

SISTEMA ATM (Asynchronous Transfer Mode). Modo de Transferencia Asíncrona, esta también es una tecnología de red diseñada para alta velocidad de transferencia de datos. ATM define una estructura física de 53 bytes, denominada celda, la cual puede ser usada para transmitir voz, datos y vídeo en tiempo real, todo sobre el mismo cable en forma simultanea.

La tecnología ATM básica viaja a 155 Mbps pero algunas versiones permiten 660 Mbps. Inclusive, en pruebas de laboratorios se han alcanzado velocidades mucho más altas. Este sistema de transmisión ha sido denominado de tercera generación debido a que se cambiaron los esquemas tradicionales de transmisión de información a través de la red.

CUADRO COMPARATIVO ENTRE DIFERENTES TOPOLOGÍAS

TOPOLOGÍA	VENTAJAS	DESVENTAJAS
Bus	• Es muy económica pues solo se necesita un cable (bus). • Los datos son compartidos por todas las terminales. • Es fácil agregar o eliminar dispositivos de la red, ya que estos están secuencialmente encadenados.	• Si el cable se daña en cualquier punto, ninguna estación podrá transmitir datos.
Arbol	• Por su topología permite que la red se expanda. • Asegura que nada mas exista una ruta de datos. • Los ETD subordinados ejercen un control en los ETD inferiores.	• Presenta muchos cuellos de botella. • Si el ordenador principal falla toda la red se incapacita. • Permite la evolución gradual hacia una red mas compleja.
Estrella	• Cubren grandes distancias al regenerarse la señal. • El mannto. Es relativamente sencillo. • El aislamiento y la recuperación de fallas es	• Vulnerable al cable. • Falla en los repetidores. • Tiempo de respuesta de acuerdo al numero de nodos. • No es muy fácil de instalar.

	sencillo.	
Anillo	• Fácil de mantener. • Fácil de conectar los componentes. • Fácil de agregar nuevos repetidores.	• La información se transmite en un solo sentido. • Si alguna terminal falla, puede hacer que toda la red se caiga.
Malla	• Es atractiva por su inmunidad a los problemas de embotellamiento y averías.	• La lógica de control de este tipo de red puede llegar a ser muy complicada. • Su costo es muy elevado.

CARACTERISTICAS Y RECOMENDACIONES

AL INSTALAR UNA RED.

Para la instalación de la red como punto de referencia existen preguntas básicas que nos den la visión general de red; que esta se toma de la respuesta de estas mismas.

- Para que se quiere o se necesita la red.
- Cuanto es el presupuesto asignado a este proyecto y que posibilidades existe de que este crezca.
- A que nivel se pretende llegar con la red y pedir la aproximación en tiempo del tipo de crecimiento de la empresa o solicitante. (En dado caso que el solicitante opinara que su red no crecerá uno como admo (De redes debe de dejar la mínima opción de expansión de la red sin avisar al solicitante)

La primera pregunta es de mucho significado en su respuesta nos da la visión de que S.O. (sistema operativo). Se puede usar para el fin; debido a que existen muchos S.O. En el mercado unos más baratos que otros y algunos son gratis como linux y sus diferentes versiones, unos son de uso mas específico que otros, más estables y multi-protocolos de comunicación entre otros S.O. A demás de que los a multi plataforma, multi usuarios y multiprocesos. Todos estos aspectos se deben de tomar en cuenta ala hora de elegir el S.O. Así como si las personas que van a usar la red tienen conocimiento en el uso del S.O.

Aquí mismo se puede tener la idea de que clase de hardware se debe de comprar como mínimo (esperando respuesta del presupuesto para saber si se puede comprar equipo mas sofisticado o de mayor calidad).

EJEMPLO 1.

Si la red se necesita solo para compartir impresoras, entonces no se necesita mucha inversión; una red de este tipo trabaja con 10 mbps. (Mbytes por segundo). Y se puede hacer con tarjetas de red ethernet que use cable del de tipo coaxial, debido que la velocidad ala que trabajan estas tarjetas y el cable coaxial tiene como un máximo de transmisión de 10 mbps. (Claro este tipo de red con este cable esta casi en desuso.)

La segunda pregunta despeja la duda de cuanto se dispone para la instalación de la red, si el presupuesto es muy bueno lo mas seguro es que no se necesite emplear un estudio costo-beneficio. Pero si el presupuesto es corto o algo limitado se debe de realizar tal estudio para tratar que el solicitante amplíe este presupuesto.

También se puede dar el caso que el solicitante pida el estudio costo-beneficio o que el admo. De red tenga que hacerlo para que se le asigne presupuesto (así que en esta uno interviene en el resultado).

La tercer pregunta. Despeja la duda de que tanto se va a crecer con la red y una aproximación en el tiempo y en el tipo de equipo en el sentido que no se vuelva obsoleto y anticuado y en caso de que no se piense crecer

por parte del solicitante uno debe de dejar esa posibilidad abierta pues por algo están asiendo la red.

CARACTERÍSTICAS DE UNA RED.

- Debe de funcionar para el fin establecido
- Debe de ser lo más estable posible.
- Contener la posibilidad de crecer (ampliarse).
- El costo debe de ser costiable por el solicitante.
- Contener velocidad de transmisión.
- Métodos de detección de errores en las tarjetas (en el caso de usar tarjetas con tecnología actual).

RECOMENDACIÓN.

- Evaluar el uso de servidor actualmente el emplear medias no son muy necesarios.
- Hacer le estudio costo beneficio para definir el presupuesto. ,
- Tipo de plataforma del software y del hardware.
- Definir su topología en algunas categorías para evaluarlas.
- Establecer métodos de protección para la red como nobreak para apagones de corriente o bajones, usar antivirus en toda la red. Etc.
- Evaluar la ergonomía física y ambiental del area y puestos de trabajos de la red en su propio diseño.
- Ver el mejor método o el mas recomendado para almacenar dado en formas de respaldos.
- Ver con que niveles de seguridad se contara en la red y que el S.O. También ofrezca esta posibilidad.

RECOMENDACIONES EN EL USO DE ALGUNA TECNOLOGÍA ACTUAL.

- En estos tiempos las tecnologías que ofrecen mejores prestaciones se han estado abaratando por la gran competencia y es mas costiable por sus beneficios el uso de la misma ejemplo:

Las tarjetas de redes existen la de 10 mbps. Y las de 10/100 mbps. Y esta ultimas son costeables pues en estos momentos su precio oscila en 200 a 250 pesos Mexicanos y las mas anticuadas andan alrededor de 120 pesos diferencias mínimas en beneficios.

OTRO EJEMPLO

Actual mente el uso del cable coaxial esta cayendo en desuso su costo es casi parecido al cable par-trenzado lo mismo pasa en los conectores las campanas y las resistencias terminatorias como se usan mas sala mas caro que los conectores RJ45. Por otro lado las redes construidas con cable coaxial cuando se cae una terminal esta afecta a todas las demás y para buscar el defecto se tienen que recorrer casi toda la red asta encontrar en que punto del cableado se daño.

Ejemplo de software y S.O. En redes mínimos:

Supongamos que el software esta hecho en modo dos un formato de 8-16 bits, esto nos indica que el mínimo de S.O. Es MS-DOS para formato de 8 bits y Windows 3.1 o 3.11 para formato de 16 bits en adelante. En caso de que el software se para un sistema de 32 bits se tendrá que usar Win95 o Win98 en adelante en el caso particular de Win NT Server o Workstation se necesita saber si el software corre en esto sistemas debido a que usan una partición NTFS pero por lo general se tiene cierta compatibilidad entre los S.O. De la casa Microsoft.

En el caso de usar Uníx o linux se usan particiones swap y por lo mismo son software que no se pueden instalar en oros S.O. Al menos que este lo permita .

EJEMPLOS

Las Imap soportan un S.O. Conocido como OS2 versión donde dise versión se especifica en numero de la versión pero para esta arquitectura linux también funciona. En el caso de la arquitectura de Silicongraphic. El S.O. Se conoce como Solarix y este tiene comunicación con Unix por protocolos en comun. El S.O. Netware de Novell este también se comunica con Unix por el protocolo TCP/IP en determinas versiones además convive con los Microsoft pues es multiplataforma y con el fin de tener servidores asignados. Lantastic de la casa arisoft usa el ms-dos y win95/98 en tipos de rede punto, punto o estrellas y atual mente distrivulle internet en toda la red con una sola cuenta apartir de la versión 7 en adelante. El S.O. Lan server de IBM. Compatible con todos los S.O. Por manejar varios protocolos cono NT y TCP/IP etc. Y su uso es de crear servidores dedicados.

Nota: son muchas la s características y recomendaciones para la instalación de una red, tanto de software, S.O. plataforma de maquinas, cableados, topologías, protocolos de comunicación y todas estas se deben de tomas en cuenta al momento de empezar su diseño para tener una RED fuerte y estable.

TELEPROCESO

ESTANDARES Y COBERTURAS, PROTOCOLOS Y TIPOLOGÍAS.