**Redes para Dummies**

Realizada por: Enrique E. Pacheco; Erick Salinas Guisell Villanueva

**Idea:** Enrique E. Pacheco

**Introducción**

Las redes en nuestro mundo actual son muy importantes ya que te pueden ayudar a economizar tanto dinero como espacio, ya que gracias a ellas puedes compartir desde un simple archivo de Word, hasta una impresora. Además de que en las grandes empresas son muy utilizadas y con esta publicación aprenderán a hacer todo lo mencionado, visto en el entorno de Microsoft ya que es uno de los OS más comunes. El libro de "Redes para Dummies" tiene el fin de instruir a los alumnos de sexto semestre en la materia de Introducción a las redes, impartida por el profesor Santiago Gachuz Miranda. En este libro se podrán apreciar todos los temas que se verán el sexto semestre en la materia ya mencionada, además, estarán representadas por imágenes para que puedan, ya sea apreciar o conocer mejor los elementos que conforman al estudio de las redes computacionales. Igualmente a lo largo de este libro se encuentran algunas prácticas ilustradas para poner en práctica todo lo teórico que se verá. Sin más preámbulo, empezamos este libro de "Redes para Dummies"

¡Saludos!

**1.- Para empezar… ¿Qué carambas es una red?**

Una red es una serie de ordenadores y otros dispositivos conectados por cables entre sí. Esta conexión les permite comunicarse entre ellos así como compartir información (documentos, imágenes, etc.) y recursos (scanner, impresora, quemador de CD o DVD).

**Red de computadoras**

**2.- Clasificación de las redes**

Hay diversos tipos de red y cada una tiene una función diferente, ya que cada una abarca diferentes espacios, a continuación veremos algunos tipos de redes:

- **Red PAN (Personal Area Network)**: O red de área personal, es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.
- **Red LAN (Local Area Network**): O red de área local, es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización. Por lo regular estas redes son baratas.
- **Red CAN (Campus Area Network):** O red de área campus, es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.
- **Red MAN (Metropolitan Area Network**): O red de área metropolitana, es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Es la unión de varias LAN.

- **Red WAN (Wide Area Network):** O red área amplia. Son redes informáticas que se extienden sobre un área geográfica extensa.
- **Red SAN (Storage Area Network)**: O red de área de almacenamiento. Es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte.
- **Red VLAN (Virtual LAN):** O red de área local virtual. Es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física.

**3.-ELEMENTOS DE UNA RED**

Una red de computadoras consta tanto de hardware como de software.

**En el hardware se incluyen:** estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad.

En **el software se encuentra** el sistema operativo de red (Network Operating System, NOS).

**Estaciones de trabajo**: Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras. Esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun, etc.

**Servidores**: Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

**Tarjeta de Interfaz de Red:** Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. Las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes. A menudo se usan cajas externas para Mac's y para algunas computadoras portátiles. La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.

**Cableado:** La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial. *Cable de par trenzado: Es con mucho, el tipo menos caro y más común de medio de red.

- **Cable coaxial**: Es tan fácil de instalar y mantener como el cable de par trenzado, y es el medio que se prefiere para las LAN grandes.
- **Cable de fibra óptica**: Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.

**Equipo de conectividad**: Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor.

- **Hubs o concentradores**: Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella.
- **Repetidores**: Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.
- **Puentes:** Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN. Repetidor *Ruteadores: Los ruteadores son similares a los puentes, sólo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring.
- **Compuertas**: Una compuerta permite que los nodos de Puente una red se comuniquen con tipos diferentes de red o con Sistema operativo de red.

**Sistema operativo de red**: Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades. Algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

**Los servicios que el NOS realiza son:**

**Soporte para archivos**: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.

**Comunicaciones**: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

**Servicios para el soporte de equipo**: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

**4.-MEDIOS DE TRANSMISION**

**Repetidores**: Dispositivo que se utiliza para propagar una señal baja

**Cables**: Pueden ser: Par trenzado, coaxial, fibra óptica, inalámbrica.

**Cable de par trenzado**. El cable de par trenzado es el tipo de cable más utilizado. Tiene una variante sin apantallar y otra con apantallamiento.

El cable de par trenzado sin apantallar, conocido como UTP (Unshielded Twisted Pair), suele ser la mejor opción para una PYME (Pequeñas y Medianas Empresas). La calidad del cable y consecuentemente, la cantidad de datos que es capaz de transmitir, varían en función de la categoría del cable. Las graduaciones van desde el cable de teléfono, que solo transmite la voz humana, al cable de categoría 5 capaz de transferir 100 Megabytes por segundo. El estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. La sigla RJ se refiere al estándar Registered Jack, creado por la industria telefónica. Este estándar se encarga de definir la colocación de los cables en su pin correspondiente. Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas.

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

Aunque la instalación de cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias, también es posible conectar distancias mayores que con los cables de par trenzado.

**Cable de fibra óptica.** El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz, con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios, debido a su inmunidad a la humedad y a la exposición solar. Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencias o servicios interactivos.

El costo es similar al cable coaxial o al cable UTP pero las dificultades de instalación y modificación son mayores.

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

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

Las desventajas de este tipo de redes son su alto costo, su susceptibilidad a las interferencias electromagnéticas y la baja seguridad que ofrecen. Además son más lentas que las redes que utilizan cableado.

**5.-MEDIOS DE CONEXIÓN**

**Panel de parcheo**: Dispositivo que permite la conexión de múltiples pares trenzados para redes de computadoras.

**Adaptadores de red**: Mejor conocido como tarjeta de red; es la comunicación entre el CPU y el modem.

**Cables**: Son los que se vieron en el tema anterior.

**6.-SOFTWARE**

Los software's que necesita una red son: EL OS, controladores de dispositivos, herramientas de diagnóstico, herramientas de corrección y optimización, servidores y utilidades.

**7.-MODELO OSI**

El modelo de interconexión de sistemas abiertos, también llamado OSI (open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

**Capas del modelo OSI:** El modelo OSI se divide en siete capas y sus funciones son:

**Capa 7. Capa de Aplicación**

Dos ordenadores se intercomunican a través de procesos, correspondiente a unas determinadas aplicaciones. El intercambio de información entre dos procesos se efectúa por medio de algún protocolo de la capa de aplicación. Algunos protocolos de la capa de aplicación son TELNET, FTP, SMTP, POP3, DNS, RTP, HTTP.

- **TELNET**: Es una aplicación que permite desde nuestro sitio y con el teclado y la pantalla de nuestro Ordenador, conectarnos a otro ordenador remoto a través de la red.
- **FTP**: Es una herramienta que te permite, a través de la red, copiar ficheros de un ordenador a otro.
- **SMTP**: Es un servicio de correo a través de servidores, usando un protocolo estándar para enviar y para recibir el correo.

- **POP3:** Protocolo POP (Protocolo de oficina de correos), permite recoger el correo electrónico en un servidor remoto.  DNS: El servicio permite, una vez configurado, que tu web y tu correo electrónico sean localizados desde cualquier lugar del mundo mediante tu nombre de dominio.
- **RTP:** (Real-Time Transfer Protocol) se utiliza para encapsular VoIP paquetes de datos dentro de paquetes UDP.
- **HTTP**: Protocolo de Transmisión Hipertexto. Protocolo de comunicaciones utilizado por los programas clientes y servidores de WWW para comunicarse entre sí.

**Capa 6. Capa de Presentación**

Trata de homogeneizar los formatos de representación de los datos entre equipos de la red.

Para homogeneizar la representación de datos (Textos, Sonidos, imágenes, valores numéricos, instrucciones), la capa de presentación interpreta las estructuras de las informaciones intercambiadas por los procesos de la aplicación y las transforma convenientemente.

Puede realizar transformaciones para conseguir mayor eficacia en la red (compresión de texto y cifrado de seguridad). Los programas del nivel 6 suelen incluirse en el propio Sistema Operativo.

La representación de los caracteres como los datos de texto y numéricos dependen del Ordenador, se representan por códigos de representación EBCDIC, ASCII y UNICODE.

**Capa 5. Capa de sesión**

Cuando se realiza una transferencia entre dos ordenadores se establece una sesión de comunicaciones entre ambos. La capa de sesión es responsable de:

- Actuar de interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre procesos remotos.
- Establecer un dialogo entre dos equipos remotos para controlar la forma en que se intercambian los datos.
- Identificar los usuarios de procesos remotos
- Cuando se corta la conexión de forma anormal, en la capa de transporte o en inferiores, la capa de sesión puede encargarse de restablecer la sesión de forma transparente al usuario.

Su función es aumentar la fiabilidad de la comunicación obtenible por las capas inferiores, proporcionando el control de la comunicación entre aplicaciones al establecer, gestionar y cerrar sesiones o conexiones entre las aplicaciones que se comunican.

**Capa 4. Capa de Transporte**

Se encarga del transporte de la información, desde la fuente al destino, a través de la red.

Los accesos a la capa de transporte se efectúan a través de puertos (sockets). EL objetivo es realizar un servicio de transporte eficiente entre procesos o usuarios finales. Para dicho fin, toma los mensajes del nivel de sesión, los distribuye en pequeñas unidades (Segmentos) y los

pasa a la red. Los protocolos de la capa de transporte se aseguran que todos los segmentos lleguen de forma correcta a su destino, para lo cual realizan detección y corrección de errores, además de controlar el flujo y la secuenciación. Otras funcionalidades es optimizar el transporte, realizando múltiplex acciones de varios mensajes en un segmento para abaratar costes.

**Capa 3. Capa de la Red.**

- Se encarga de Fragmentar los segmentos que se transmiten entre dos equipos de datos en unidades denominadas paquetes. En el ordenador receptor se efectúa el proceso inverso: los paquetes se ensamblan en segmentos.
- Realizar el encaminamiento de los paquetes. Se encargará de realizar algoritmos eficientes para la elección de la ruta más adecuada en cada momento, para reexpedir los paquetes en cada uno de los nodos de la red que deba atravesar.
- Prevenir la producción de bloqueos así como la congestión en los nudos de la red de transporte que pudiesen producirse en horas punta por la llegada de paquetes en forma masiva.

**Capa 2. Capa de enlace de datos**

Descompone los mensajes que recibe del nivel superior en tramas o bloques de información, en las que añade una cabecera (DH) e información redundante para control de errores. La cabecera suele contener información de direcciones de origen y destino, ruta que va a seguir la trama, etc.… También se encarga de transmitir sin error las tramas entre cada enlace que conecte directamente dos puntos físicos (nodos) adyacentes de la red, y desconectar el enlace de datos sin pérdidas de información.

**Capa 1. Capa Física**

Es donde se especifican los parámetros mecánicos (grosor de los cables, tipo de conectores), eléctricos (temporizador de las señales, niveles de tensión) de las conexiones físicas. Las unidades de información que considera son bits, y trata de la transmisión de cadenas de bits en el canal de comunicación (pares trenzados de cobre, cable coaxial, radio, infrarrojos, Wifi, fibra óptica), si el emisor envía un 0, al receptor debe de llegar un 0.

**8.-PROTOCOLOS COMUNES**

Conjunto de reglas usadas por computadora para comunicar una red con otra.

**Sus características son**:

- **El protocolo CSMA/CD (Carrier Sense Multiple Access, Collision Detection)** Verifica que la línea este libre y al enviarlo revisa que no haya conexiones, es decir, este protocolo solo detecta la colisión de información (choque de datos) cuando ya ocurrió.
- **El protocolo CSMA/CA (Carrier Sense Multiple Access, Collision Avoidance)** A diferencia del CSMA/CD este, trata de evitar la colisión de la información, primero se asegura que la red este libre y luego manda la información.
- **Los métodos de protocolos son:**

- **Protocolos por poleo**: Se caracteriza por contar con un dispositivo controlador central que es una computadora inteligente como un servidor.
- **Paso de testigo en anillo**: Emplea un testigo para autorizar la transmisión de quien lo posea.
- **Protocolos de contención**: No hay nadie que controle el uso de los canales de comunicación. Basado en que el primero que llega es el que utiliza la línea.
- **Contención simple**: Los mensajes que se van a transmitir convierten en paquetes y se envían cuando estén listos.
- **Los protocolos ESMA**: Persistente y no persistente representan verdaderamente una mejora al sistema.

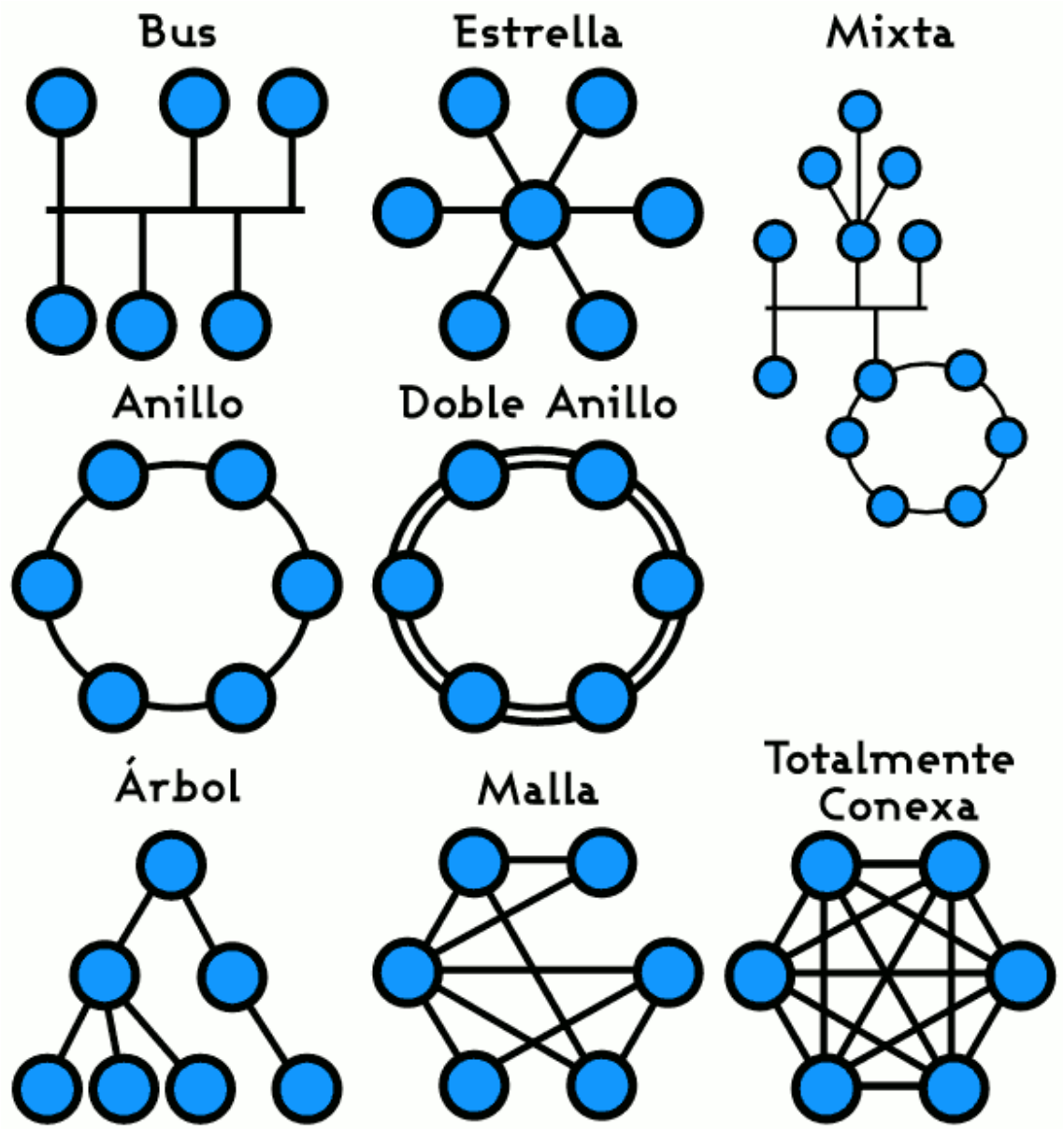
**Los protocolos más comunes son: TCP/IP** (usado en empresas y está basado en Internet), **IPX** (Esta orientado a comunicación sin conexión), **SPX** (Necesita cableado y consiste en paquetes en secuencia), **Apple talk** (Conjunto de protocolos para conexión de redes MAC), **Netbeui** (Primeras capas en las redes de Microsoft) y la **Norma IEEE 802** (Reglas para estar en Internet)

**9.-TOPOLOGIAS**

Se define como la forma de tender a un cable a estaciones de trabajo individuales.

**Una topología se divide en:**

**Física:** Ubicación de cada uno de las maquinas en red.




**Lógica**: Referencia a la forma de comunicarse para transferir la información. Hay diferentes tipos de topologías las cuales son: **Anillo, bus, árbol, estrella, malla e híbrida**. Para que se entiendan mejor se explicara su definición, algunas ventajas y desventajas de la topología y el cable que utilizan. Cabe mencionar que cuando se menciona el cable coaxial va a ir siempre con un conector RJ45, como se vio en temas anteriores, y cuando se menciona un cable par trenzado se utilizará siempre el conector BNC.

**Red en anillo**

Cada conexión está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente acción. La señal va pasando en círculo y cada máquina debe esperar su turno para solicitar o recibir información. El cable que utiliza es el coaxial.

**Ventajas**

- Simplicidad en la arquitectura
- Facilidad de fluidez de datos

**Desventajas**

- Longitud de canales
- El canal se degrada a medida que la red crece.

**Red en bus**

Único canal de comunicaciones al cual se conectan los diferentes dispositivos. Todos estos dispositivos comparten el mismo canal. Los extremos usan una resistencia de acople llamada terminador. Es una topología pasiva.

**Ventajas**

- Facilidad de implementación y crecimiento.
- Simplicidad de arquitectura.

**Desventajas**

- Límite de equipos dependiendo de la calidad de la señal.
- Degradación de la señal.
- Complejidad de configuración y almacenamiento de fallos.
- Limitación de longitudes.
- Desempeño disminuye a medida que la red crece.
- Altas perdidas en la transmisión debido a las colisiones entre mensajes.
- Ocupa mucho espacio.

**Red en árbol**

Los nodos están en forma de árbol, no tiene un nodo central, la falla en un nodo no implica la interrupción en las comunicaciones. Requiere un cable coaxial.

**Ventajas**

- El hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la inclusión de concentradores secundarios.
- Se pueden conectar más dispositivos gracias a la inclusión de concentradores secundarios

**Desventajas**

- Los datos son recibidos por todas las estaciones sin importar para quien vayan dirigidos.
- Interferencia.
- Muchos cables.
- Difícil configuración.
- Si se viene abajo el segmento principal todo el segmento se va con él.

**Red en estrella**

Las estaciones están conectadas directamente a un punto central, todas las comunicaciones se hacen a través de éste; los dispositivos no están directamente conectados entre sí; no se permite tanto tráfico de información. Requiere un cable par trenzado.

**Ventajas**

- Sí una PC se desconecta o rompe el cable, solo queda fuera de la red esa PC.
- Fácil de prevenir daños o conflictos.

Desventajas

- Sí el servidor atrapa un virus, toda la red lo atrapa.
- Sí el nodo central falla, todo falla
- Costosa.

**Red en malla**

Cada nodo está conectado a todos los nodos; es posible llevar mensajes de un nodo a otro por diferentes caminos; Sí la red de malla está completamente conectada, no hay ninguna interrupción en las comunicaciones; cada servidor tiene sus propias conexiones con todos los demás servidores; no hay servidor o nodo central; son auto ruteables. El cable que utiliza es el par trenzado.

**Ventajas**

- Llevar información de un nodo a otro por diferentes caminos.
- Sí falla un cable el otro se hará cargo del tráfico.
- Si un nodo falla no pasa nada.

**Desventajas**

- Caras
- Mucho cable.

**Red híbrida**

Acerca de esta topología solo se puede decir que es la combinación de dos o más topologías. Usará igualmente el cable y conector de cada una de las topologías.

**Ventajas**

- Las ventajas dependen de las redes que estén unidas.

**Desventajas**

- Mucho cable.
- Desventajas de cada una de las topologías.

**10.- TECNICAS DE TRANSMISION**

Pueden ser de dos tipos:

- Guiados
- No guiados

Los guiados son por medio de cables. Y los no guiados puede ser por una banda ancha o una banda base (describe el estado de la señal).

**11.- INTERCONEXIÓN**

**Red Ethernet:** Una red Ethernet es un tipo partículas de cableado de red, más específicamente, de señalización que cubre las capas 1y2 del modelo OSI. En una red de banda base; o sea, que provee un único canal de comunicación sobre el medio físico (cable), de modo que solo puede usarlo un dispositivo a la vez. Ethernet usa el protocolo CSMA/CD.

**Arquitectura Token-Ring:** La red Token-Ring es una implementación del estándar IEEE 802.5 en el cual se distinguen más por su método de transmitir la información que por la forma en que se conectan las computadoras. El 1er diseño de una red de Token-Ring es atribuido a EE. Newhall en el '69. IBM publicó por 1ª vez su topología de TokenRing en marzo de 1982, el proyecto 802 del IEEE. IBM anunció un producto Token-Ring en el '84, y en el '85 llegó a ser un estándar de ANSI/IEEE.

**Apple Talk**: La arquitectura de red de Apple está incluida en el software de OS de Macintosh. Esto quiere decir que las capacidades de red están incluidas en cada Macintosh. Cosas que pasan cuando se conecta una red Apple talk:

1 El dispositivo comprueba si hay guardada una dirección de una sesión de red anterior.

2 El dispositivo informa de la dirección para comprobar si hay otro dispositivo utilizándola.

3 Si no hay otro dispositivo utilizando la dirección, el dispositivo queda guardado para después utilizarla.

**Redes FDDI**: Es la más reciente tecnología en redes de datos, sus características se encuentran establecidas por el estándar FDDI ANSI X 3T9 de la ANSI, FDDI, viene a ser la interface para datos de fibra distribuida, se basa en el uso de la fibra óptica.

**12.- NORMA 568a y 568b**

| Número de PIN | Norma 568ª | Norma 568b |
|---|---|---|
| 1 | Blanco-Verde | Blanco-Naranja |
| 2 | Verde | Naranja |
| 3 | Blanco-Naranja | Blanco-Verde |
| 4 | Azul | Azul |
| 5 | Blanco-Azul | Blanco-Azul |
| 6 | Naranja | Verde |
| 7 | Blanco-Café | Blanco-Café |
| 8 | Café | Café |

## 13.- PROCESO DE CONFIGURACIÓN DE UNA RED MICROSOFT

- **Creación de grupos de trabajo.**

a) El grupo de trabajo indica el nombre de la red a la que se va a tener acceso o bien la que se va a crear.

Para establecer los grupos de trabajo es necesario considerar lo siguiente para el nombre: No utilizar símbolos o caracteres especiales, ni espacios para el nombre.

Para crear el grupo de trabajo se debe llevar a cabo el siguiente proceso:

1.- Activar la ventana para la creación (presionando el botón Windows más la tecla pause del teclado)

2.- Entrar a la ficha de "nombre del equipo"

3.-Hacer clic en el botón "cambiar", y en el nombre de equipo asignar uno considerando no poner espacios en blanco ni caracteres especiales.

4.- Asignar el nombre del grupo de trabajo.

5.-Se da clic en aceptar y el equipo pedirá que reinicies el equipo, reinícialo.

6.-Cuando se haya reiniciado accedes al menú inicio y buscas la opción, "mis sitios de red".

7.- Abrir los equipos conectados al grupo de trabajo o "ver equipos de grupo de trabajo".

## 14.- COMPARTIR RECURSOS EN RED

Se va a explicar el proceso básico para compartir los recursos de red; sin entrar a configuración de permisos y restricciones del acceso a dichos recursos en Windows 2000, Windows XP y Windows 7.

1.- Los PC's que van a formar parte de la red, ya están conectados entre sí, y se han configurado los parámetros del TCP/IP, etc.

2.-Configuracio inicial: Hay que comprobar que estén instalados tanto el cliente para redes de Microsoft como el servicio a compartir archivos e impresoras para redes Microsoft.

3.-Compartiendo recursos de red: Para poder acceder a recursos de otros equipos, hay que compartirlos primero, ya sea un disco duro, carpeta o impresora.

## 15.-CABLEADO Y CONECTORIZACIÓN

### Modelo cliente servidor

Considera la presencia de un servidor dedicado (una computadora que hace el único papel de servidor) y personal calificado.

El modelo de estrella exige la instalación de un RACK de comunicación a donde llegan todos los cables de interconexión y se conectará el servidor.

**Las actividades a realizar son:**

- Definir, diseñar y construir el espacio donde se ubicará el administrador de la red y el rack.
- Definir las características del servidor y adquirirlo.
- Definir trayectorias del cableado y cuantificar elementos necesarios tales como, cajas, canaletas y paneles de parcheo.
- Etiquetar el cableado
- Llevar a cabo la instalación del cableado y realizar pruebas de interconexión

**16.- CONSIDERACIONES PARA LA INSTALACION DE UNA LAN**

- **Pérdida de datos**: Es producida por algún virus u otro tipo de incidencia, o personas inescrupulosas que acceden al sistema mediante Internet, pueden evitarse con firewalls que sirve para detener los intrusos.
- **Caídas continuas de la red**: Se debe a una mala conexión servidor > concentrador.
- **Proceso de información len**ta: Cuando el procesamiento de información es muy lento tenemos que tomar en cuenta el tipo de equipo que elegimos.

**Protocolos a usar**

**TCP/IP**: Trabajan juntos para transmitir datos:

Cuando envías información los datos se fragmentan en pequeños paquetes. El protocolo de control de transmisión divide los datos en paquetes y los reagrupa cuando se reciben.

**Norma EIA/TIA568**: ANSI/ TIA/ EIA-568-A (alambrado de telecomunicaciones para edificios comerciales).

El propósito es permitir el diseño e instalación del cableado contando con poca información acerca de los productos que posteriormente se instalarán.

**Alcance**: La norma EIA/ TIA 568-A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas.

- Las topologías
- Distancias de cables

El cableado tiene que soportar varios tipos de edificios y aplicaciones de usuario:

- Distancia máxima de 3 metros.
- Espacio de oficina de un millón de metros cuadrados.
- Población hasta 50’000 usuarios.

Las aplicaciones que emplean no están limitadas a:

- Voz, datos, texto, video e imágenes.

La vida útil de los sistemas del cableado debe ser mayor a 10 años.

**Beneficios:** Flexibilidad, asegura compatibilidad de tecnologías, reduce fallas, traslado, adiciones y cambios rápidos.

**PONCHADOR O NEXT CRIMPING TOOL RJ45**. Pasos a seguir para construir la red.

- Diseñar la red.
- Determinar el tipo de hardware de cada equipo.
- Elegir el host (Computadora de la cual se va a usar a algún recurso).
- Determinar el tipo de adaptador de red.
- Lista de hardware a comprar.
- Medición del espacio entre estación de trabajo y host
- Colocación de canaletas plásticas.
- Medición del cableado.

**17.- COMO COMPARTIR UNA IMPRESORA. (Ejemplo Windows XP)**

1.- Se presiona el botón de inicio y en el menú se selecciona impresoras y faxes, si no aparece, dirigirse a panel de control y ahí buscar impresoras y faxes.

2.- Al acceder se selecciona la opción “agregar una impresora”

3.- seguir los pasos de instalación como se ve en las imágenes.

Esperar hasta que aparezca la computadora que tiene la impresora, seleccionarla y presionar siguiente; ¡listo!

**18.- DIRECCIONES IP**

Una **dirección IP** es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar. A esta forma de asignación de dirección IP se denomina dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática), esta, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

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

**19.- ADMINISTRACIÓN DE RED**

Abarca un amplio número de asuntos. En general se suele tratar con muchos datos estadísticos e información sobre el estado de distintas partes de la red, y se realizan las acciones necesarias para ocuparse de fallos y otros cambios. La técnica más primitiva para la monitorización de una red es hacer "PINGING" a los host críticos; el "PINGING" se basa en un datagrama de echos (ecos), que es un tipo de datagrama que produce una réplica inmediata cuando llega al destino. La mayoría de la implementaciones TCP/IP incluyen un programa (generalmente llamado "PING") que envía un echo a un host en concreto. Si recibimos réplica, sabemos que host se encuentra activo, y que la réplica que los conecta funciona; en caso contrario, sabremos que hay algún error. Mediante "PINGING" a razonable número de ciertos hosts, podremos normalmente conocer que ocurre en la red.

Si los PING a todos los hosts de una red no dan respuesta es lógico concluir que la conexión a dicha red o la propia red no funcionan. Si solo uno de los hosts no da respuesta, pero los demás de la misma red responden, es razonable concluir que dicho host no funciona.

Técnicas más sofisticadas de monitorización necesita conocer información estadística y el estado de varios dispositivos de la red. Para ello necesitara llenar la cuenta de varias clases de datagramas, así como de errores de varios tipos. Este tipo de información será más detallada en los Gateways, puesto que el Gateway clasifica los datagramas según protocolos e incluso, él mismo responde a ciertos tipos de datagramas. Sin embargo, los bridges e incluso los repetidores con buffer contabilizan los datagramas reenviados, errores de interface. Es posible recopilar todo esta información en un punto de monitorización central.

También hay un enfoque oficial **TCP/IP** para llevar a cabo la monitorización. En la primera fase, usamos un conjunto de protocolos **SGMP y SNMP**, ambos diseñados para permitirnos recoger información y cambiar los parámetros de la configuración y otras entidades de la red. Podemos ejecutar los correspondientes programas en cualquier host de nuestra red. SGMP está disponible para varios gateways comerciales, así como para sistemas UNIX que actúan como Gateway. Cualquier implementación SGMP necesita que proporciones un conjunto de datos para que pueda empezar a funcionar y tiene mecanismos para ir añadiendo informaciones que varían de un dispositivo a otro. A finales de 1988 apareció una segunda generación de este protocolo, **SNMP** que es ligeramente más sofisticada y necesita más información para trabajar y, para ello, usa el llamado **MIB (Management Information Base).** En lugar de usar una conexión de variable **SNMP**, **el MIB es** el resultado en numerosas reuniones de comités formados por vendedores o usuarios. También se espera la elaboración de equivalente de **TCP/IP de CMIS.**

En términos generales, todos estos protocolos persiguen el mismo objetivo: Permitirnos recoger información crítica de una forma estandarizada. Se ordena la emisión de datagramas UDP desde un programa de administración de redes que se encuentra ejecutando en algunos de los hosts de red.

Probablemente queremos configurar la administración de la red con las herramientas que tenemos a nuestra disposición pero controlar diversas actividades. Es posible configurar SGMP, SNMP para que use “trabs” (mensajes no solicitados) para un host en particular o para una lista de host cuando ocurre un evento crítico. También es posible que los mensajes “trabs” se pierdan por un fallo en la red o por sobrecarga así que no podemos depender completamente de los “trabs”. Otro tipo de monitorización deseable es recolectar información para hacer informes periódicos del porcentaje del uso de la red y prestaciones. Sería posible que cualquier tipo de conmutador pudiese usar cualquier tipo de técnica de monitorización. Los gateways en la mayoría de los casos incluyen un avanzado software de administración de redes. Excepto para algunas pequeñas redes, debimos insistir en que cualquier dispositivo conmutador este completo, un simple repetidor es capaz de recolectar estadísticos.

# Clases de red

| Clase | Dirección de Red | Dirección de Host | Cantidad de Hosts |
|---|---|---|---|
| Clase A | *a* | *b.c.d* | 16777214 |
| Clase B | *a.b* | *c.d* | 65534 |
| Clase C | *a.b.c* | *d* | *254* |

| **Clase** | **Tamaño de la dirección de red (en octetos)** | **Primer número** | **Número de direcciones locales** |
|---|---|---|---|
| A | 1 | 0 -127 | 16.777.216 |
| B | 2 | 128 -191 | 65.536 |
| C | 3 | 192 -223 | 256 |

Dada una dirección IP, puede determinarse a que clase pertenece examinando el valor de su primer número:

| Clase | Rango de *a* |
|---|---|
| Clase A | *1 - 126* |

| | |
|---|---|
| Clase B | *128 - 191* |
| Clase C | *192 - 224* |

Para una mejor organización en el reparto de rangos las redes se han agrupado en cuatro clases, de manera que según el tamaño de la red se optará por un tipo u otro.

## Las direcciones de clase A

La clase A comprende redes desde 1.0.0.0 hasta 127.0.0.0. El número de red está en el primer octeto, con lo que sólo hay 127 redes de este tipo, pero cada una tiene 24 bits disponibles para identificar a los nodos, lo que se corresponde con poder distinguir en la red unos 1.6 millones de nodos distintos.

## Corresponden a redes que pueden direccionar hasta 16.777.214 máquinas cada una.

Las direcciones de red de clase A tienen siempre el primer bit a 0.

0 + Red (7 bits) + Máquina (24 bits)

Solo existen 124 direcciones de red de clase A.

**Ejemplo:**

| | **Red** | **Máquina** | | |
|---|---|---|---|---|
| Binario | 0 0001010 | 00001111 | 00010000 | 00001011 |
| Decimal | 10 | 15 | 16 | 11 |

**Rangos**(notación decimal):

1.xxx.xxx.xxx - 126.xxx.xxx.xxx

## Las direcciones de clase B

La clase B comprende redes desde 128.0.0.0 hasta 191.255.0.0; siendo el número de red de 16 bits (los dos primeros octetos. Esto permite 16320 redes de 65024 nodos cada una.

## Las direcciones de red de clase B permiten direccionar 65.534 máquinas cada una.

Los dos primeros bits de una dirección de red de clase B son siempre 01.

01 + Red (14 bits) + Máquina (16 bits)

Existen 16.382 direcciones de red de clase B.

**Ejemplo:**

| | **Red** | | **Máquina** | |
|---|---|---|---|---|
| Binario | 10 000001 | 00001010 | 00000010 | 00000011 |
| Decimal | 129 | 10 | 2 | 3 |

**Rangos**(notación decimal):

128.001.xxx.xxx - 191.254.xxx.xxx

## Las direcciones de clase C

Las redes de clase C tienen el rango de direcciones desde 192.0.0.0 hasta 223.255.255.0, contando con tres octetos para identificar la red. Por lo tanto, hay cerca de 2 millones de redes de este tipo con un máximo de 254 nodos cada una.

## Las direcciones de clase C permiten direccionar 254 máquinas.

Las direcciones de clase C empiezan con los bits 110

110 + Red (21 bits) + Máquina (8 bits)

Existen 2.097.152 direcciones de red de clase C.

**Ejemplo:**

| | **Red** | | | **Máquina** |
|---|---|---|---|---|
| Binario | 110 01010 | 00001111 | 00010111 | 00001011 |
| Decimal | 202 | 15 | 23 | 11 |

**Rangos**(notación decimal):

192.000.001.xxx - 223.255.254..xxx

## Las direcciones de 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 cuatro primeros bits de una dirección de clase D son 1110.

## Comprenden las direcciones entre 224.0.0.0 y 254.0.0.0, y están reservadas para uso futuro, o con fines experimentales. No especifican, pues, ninguna red de Internet.

## Direcciones de red reservadas

Cuando se creó Internet y se definió el protocolo IP, al desarrollar los conceptos de clases A, B y C se reservaron una red clase A (10.X.X.X), quince clases B (172.16.X.X a 172.31.X.X) y 255 clases C (192.168.0.X a 192.168.255.X) para su uso privado. Este uso privado consiste en que el órgano competente en la asignación de direcciones no concede estas clases, y se reservan para que las redes privadas sin conexión con el mundo exterior hagan uso de ellas de tal manera de no provocar colisiones si en el futuro estas redes se conectan a redes públicas.

De esta forma se definen dos tipos de direcciones IP, direcciones IP públicas, que son aquellas que conceden los organismos internacionales competentes en esta materia y que van a ser usadas en Redes IP Globales, y direcciones IP privadas, definidas como aquellas que van a identificar a los equipos cuando se hable de Redes IP Privadas.

**Existen una serie de direcciones IP con significados especiales.**

- Direcciones de subredes reservadas:

000.xxx.xxx.xxx (1)

127.xxx.xxx.xxx (reservada como la propia máquina)

128.000.xxx.xxx (1)

191.255.xxx.xxx (2)

192.168.xxx.xxx (reservada para intranets)

223.255.255.xxx (2)

- Direcciones de máquinas reservadas:

xxx.000.000.000 (1)

xxx.255.255.255 (2)

xxx.xxx.000.000 (1)

xxx.xxx.255.255 (2)

xxx.xxx.xxx.000 (1)

xxx.xxx.xxx.255 (2)

1. Se utilizan para identificar a la red.
2. Se usa para enmascarar.