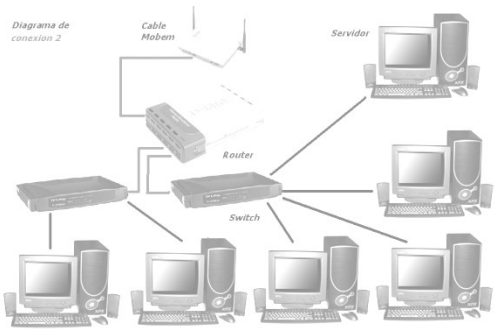
INTRODUCCION A REDES

Notas de la Materia

M.A. Mónica Hernández Barrera

Profesor



ACADEMIA DE INFORMÁTICA

Facultad de Contaduría y Ciencias Administrativas

Universidad Michoacana de San Nicolás de Hidalgo

UNIDAD I
INTRODUCCIÓN

- Definición de red
- Clasificación de las redes
- Características de las redes
- Modelos de redes

DEFINICIÓN DE RED

Una red es un conjunto de equipos informáticos interconectados entre sí.

En toda red, hay una parte física y otra parte lógica. La parte física, está compuesta por todos los elementos materiales (hardware), y los medios de transmisión. La parte lógica (software), son los programas que gobiernan o controlan esa transmisión y la información o datos que es transmitida.

Compartición de recursos

Una red de computadoras permite compartir información y recursos a los usuarios de la red.

Principales recursos para compartir:

- Unidades de almacenamiento.
- Servidor de aplicaciones.
- Impresoras.
- Acceso a internet.

CLASIFICACIÓN DE LAS REDES

- Por su tecnología de transmisión
- Por su tamaño
- Por su topología

Por su tecnología de transmisión

- Redes de difusión o broadcast
- Redes punto a punto

Redes de difusión o broadcast

En las redes broadcast hay un único canal de comunicación, compartido por todas las computadoras.

Las computadoras envían mensajes, que llegan al resto de las computadoras de la red.

Los protocolos que se utilizan en estas redes deben permitir determinar cuándo un mensaje se envía a todas las computadoras o cuándo lo hacen únicamente a una.

Los protocolos, deben preocuparse de controlar que no se produzcan colisiones.

En el mensaje, se indica el origen y el destino de dicha información.

En estas redes, el problema principal, es la asignación del canal. Para solucionar esto, hay dos métodos: asignación estática y asignación dinámica.

Asignación estática

Usa la multiplexación, para dividir el ancho de banda del canal entre las computadoras que lo usan.

Este sistema de asignación permite que cada computadora no dependa del resto para comunicar aunque, se pueden desaprovechar los canales.
Su mayor ventaja es que se evitan las interferencias y colisiones.

Asignación dinámica

Permite gestionar la utilización de un único medio en función de las necesidades de comunicación de los equipos en cada momento. Reparte el ancho de banda más eficazmente.

Se han creado distintos protocolos de acceso al medio, en redes Ethernet uno de los protocolos más usados, es CSMA/CD (Carrier Sense Multiple Access with Collision Detection). La computadora que quiere transmitir, examina si el canal lo está usando otra, en este caso espera para transmitir. Si hubiera un choque, la transmisión se detendría. El conjunto de normas IEEE 802.3, siguen este protocolo.

Redes punto a punto

Las conexiones son punto a punto, entre pares de computadoras. Se establece una comunicación directa entre las dos computadoras.

Hasta que un mensaje llega a su destino, puede pasar por varios nodos intermedios.

Dado que normalmente, existe más de un camino posible, hay algoritmos de encaminamiento (routing), que lo gobiernan.
Este tipo de redes, usa dos tecnologías diferentes: Conmutación de circuitos y conmutación de paquetes.

Conmutación de circuitos
Se establece un "circuito" entre los dos puntos, mientras dura la conexión.
Se establece una comunicación dedicada entre los nodos. El camino queda fijado durante toda la llamada, se transmitan o no datos. El circuito de llamada se establece de manera similar a una llamada telefónica y se comporta como un circuito dedicado, aunque solo mientras dura la conexión.

Ventajas

- **La transmisión se realiza en tiempo real**, siendo adecuado para comunicación de voz y video.
- **Acaparamiento de recursos**. Los nodos que intervienen en la comunicación disponen en exclusiva del circuito establecido mientras dura la sesión.
- **No hay contención**. Una vez que se ha establecido el circuito las partes pueden comunicarse a la máxima velocidad que permita el medio, sin compartir el ancho de banda ni el tiempo de uso.
- **El circuito es fijo**. Dado que se dedica un circuito físico específicamente para esa sesión de comunicación, una vez establecido el circuito no hay pérdidas de tiempo calculando y tomando decisiones de encaminamiento en los nodos intermedios. Cada nodo intermedio tiene una sola ruta para los paquetes entrantes y salientes que pertenecen a una sesión específica.

Desventajas

- **Retraso en el inicio de la comunicación**. Se necesita un tiempo para realizar la conexión, lo que conlleva un retraso en la transmisión de la información.
- **Bloqueo de recursos**. No se aprovecha el circuito en los instantes de tiempo en que no hay transmisión entre las partes. Se desperdicia ancho de banda mientras las partes no están comunicándose.
- **El circuito es fijo.** No se reajusta la ruta de comunicación, adaptándola en cada posible instante al camino de menor costo entre los nodos.
- **Poco tolerante a fallos.** Si un nodo intermedio falla, todo el circuito *se viene abajo*.

Conmutación de paquetes

En las que el mensaje se divide en partes, denominadas paquetes, que se envían independientemente unos de otros, incluso desordenados y por distintos caminos, hasta su destino, donde se debe reordenar y recomponer el mensaje.

Ventajas

- Si hay error de comunicación se retransmite una cantidad de datos aun menor que en el caso de mensajes.
- **En caso de error en un paquete solo se reenvía ese paquete**, sin afectar a los demás que llegaron sin error.
- **Comunicación interactiva**. Al limitar el tamaño máximo del paquete, se asegura que ningún usuario pueda monopolizar una línea de transmisión durante mucho tiempo.
- Se alternan diferentes caminos.

- Se pueden asignar prioridades a los paquetes de una determinada comunicación.

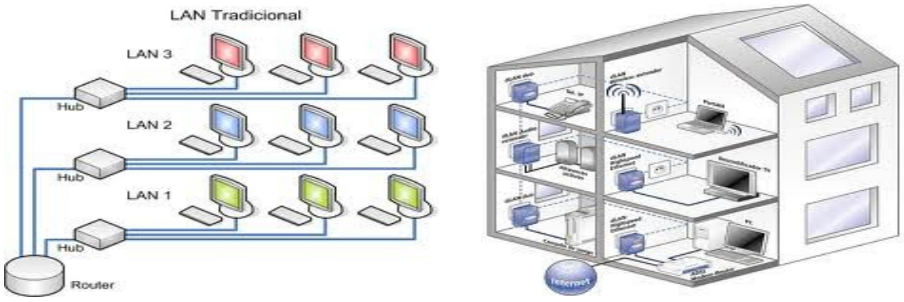
Desventajas

- **Mayor complejidad en los equipos de conmutación intermedios**, que necesitan mayor velocidad y capacidad de cálculo para determinar la ruta adecuada en cada paquete.
- **Duplicidad de paquetes**. Si un paquete tarda demasiado en llegar a su destino, el host receptor(destino) no enviara el acuse de recibo al emisor, por el cual el host emisor al no recibir un acuse de recibo por parte del receptor este volverá a retransmitir los últimos paquetes del cual no recibió el acuse, pudiendo haber redundancia de datos.
- Si los cálculos de encaminamiento representan un porcentaje apreciable del tiempo de transmisión, el rendimiento del canal (información útil/información transmitida) disminuye.

Por su Tamaño

- Redes de área local (LAN)
- Redes metropolitanas (MAN)
- Redes de área extensa (WAN)

Redes de área local(LAN)

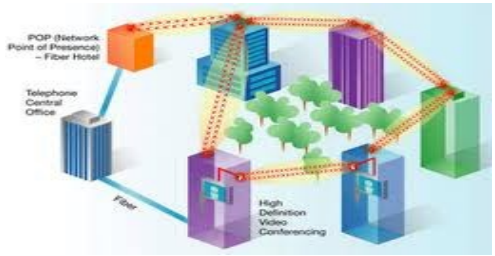


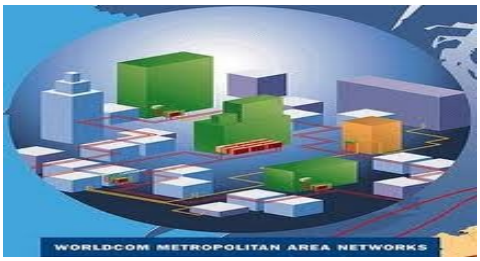
Son redes privadas con un medio físico de comunicación propio. Se consideran restringidas a un área geográfica determinada: centro docente, empresa, etc. Aunque puedan extenderse en varios edificios empleando distintos mecanismos y medios de interconexión.

La longitud máxima de los cables, que unen las computadoras, puede ir desde 100 metros, con cable de par trenzado, hasta algunos kilómetros en segmentos unidos por fibra óptica. Son redes optimizadas: permiten una gran rapidez y fiabilidad a la hora de transmitir datos.

Las computadoras comparten un mismo medio de comunicación: Todos están conectados a un medio común, por lo que para su utilización deben competir por él. Son redes de difusión: al disponer de un medio compartido pueden enviar mensajes al resto de los equipos de forma simultánea.

Redes metropolitanas (MAN)





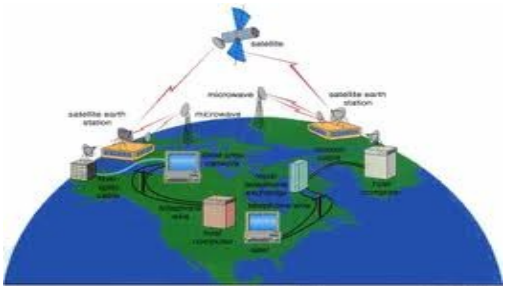
Es similar en su estructura y funcionamiento a las LAN, pero ocupan una mayor extensión geográfica y pueden ser públicas o privadas.

No necesitan elementos de conmutación y dirigen la información empleando dos cables unidireccionales, es decir,un bus doble en el que cada uno de los cables opera en direcciones opuestas.

En este tipo de redes no se pueden producir colisiones ya que no es un medio compartido, sino que se procuran métodos para el control de acceso al medio, los generadores de tramas emiten de forma regular una estructura de trama que permite la sincronización de los equipos a la hora de transmitir, ya que podrán acceder al medio cuando un contandor interno (sincronizado por la trama enviada por el generador) se ponga a cero.

Cada nodo recibe la información por un bus de los nodos posteriores y envía por el otro, de manera que puede estar emitiendo y recibiendo información de forma simultánea.

Redes de área extensa (WAN)



Consisten en computadoras y redes de área local y metropolitanas, unidas a través de grandes distancias, conectando equipos y redes a escala nacional o internacional.

La comunicación se consigue mediante routers (encaminadores) y en algunos casos gateways (llamados también convertidores de protocolos o pasarelas).

Sus velocidades de transmisión son lentas comparadas con redes de área local. Tienen una alta tasa de errores, necesitando sistemas de detección y recuperación de errores. Permiten la posibilidad de reconfiguración de las redes debido a su menor fiabilidad. Usan técnicas de almacenamiento y reenvío (Store and Fordward) en los nodos de comunicación.

Están compuestas por un conjunto de nodos interconectados donde los datos son encaminados a través de los mismos desde un emisor hasta el receptor. La comunicación entre los nodos se puede establecer mediante algún sistemas de conmutación.

Por su topología

Esa estructura puede ser física o lógica.

Topología física, la distribución física del cableado y los elementos físicos, y su forma de interconexión.

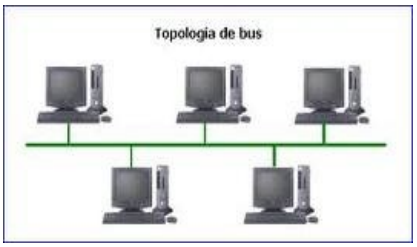
Topología lógica, la forma de circulación y la regulación de la información.

Además del cable, que es el medio físico tradicional de transmisión de datos, también puede conseguirse la comunicación, por radio, infrarrojos o microondas, son las comunicaciones inalámbricas.

Por su topología física:

- *En bus*
- *De anillo*
- E*n estrella*
- *En malla*
- *De red celular*

Red en bus



Características:

- Todos los dispositivos están unidos a un cable continuo, a través de interfaces físicas, llamadas tomas de conexión, hay terminales a cada extremo del bus para que las señales no se reflejen y vuelvan al bus.
- El cable puede ir por el piso, techo, etc., pero siempre será un segmento continuo.
- Las computadoras se unen al cable mediante unos transceptores, que pueden estar integrados en la propia tarjeta adaptadora de red.
- Los mensajes circulan en ambas direcciones.
- No hay ningún nodo central que controle la red.
- La información se transmite por todo el bus. Por ello, todos los nodos del bus pueden escuchar las señales (mensajes broadcast).

- Para evitar que varias estaciones accedan a la vez al canal o bus, se usan protocolos de acceso al bus y detección de colisiones.

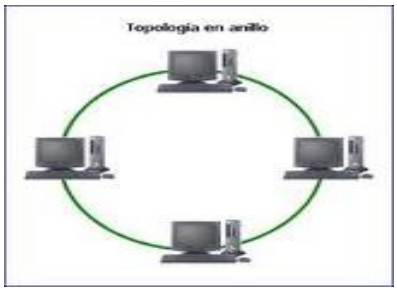
Ventajas:

- Su sencillez y bajo coste. Sólo se tiene que instalar un cable y los adaptadores.
- Este tipo de redes puede segmentarse mediante repetidores, aumentando su seguridad, independizando cada segmento y ampliando su longitud y número de nodos en la red, si bien tiene la limitación de la atenuación de la señal.
- El software de comunicaciones no necesita incluir algoritmos de routing.

Desventajas:

- La rotura del cable principal dejaría sin servicio a todos los dispositivos de la red.
- Típicas redes de este tipo son las primeras Ethernet; los otros dos son Thicknet (red gruesa, con cable coaxial 10Base5) y Thinnet (red delgada, utiliza 10Base2).

Red en anillo



Características:

- La transmisión de información es por conmutación de paquetes. Circula en una sola dirección.
- Cada nodo transmite o recibe un paquete.

- Cualquier nodo puede recibir el paquete que circula por el anillo, si es paraél, se lo queda, si no, lo pasa al siguiente.
- No hay principio ni final.
- No hay ningún nodo central que controle la red.

Ventajas:

- *Localización de errores fácil.*
- El software es sencillo, no necesita algoritmos de encaminamiento o routing.

Desventajas:

- El fallo de un enlace provoca el fallo de todo el anillo.
- Difícil adición de nodos.
- El repetidor de cada nodo ralentiza la velocidad de transmisión.
- Instalación del cableado compleja.
- Redes de este tipo son Token Ring (norma 802.5), que utiliza par trenzado como cable y FDDI (Fiber Distributed Data Interface) sobre fibra óptica.

Red en estrella

Características:

- En este tipo de redes, está formado por un nodo central al cual están

conectadas todas las computadoras de la red.

- El nodo central puede tener dos formas de funcionamiento; como repetidor de las tramas que le llegan ó repetir las tramas solamente al destino

Ventajas:

- Fácil administración.
- Sencillo añadir/desconectar nuevos nodos.

Desventajas:

- Si se avería el nodo central, no funciona la red.
- Hay que instalar una línea para cada nodo.
- La entrada /salida del nodo central puede convertirse en un cuello de botella.

Red en malla

Características:

- Los nodos de la red tienden a conectarse con el resto, de la manera más corta.
- Esta topología permite que la información circule por varias rutas alternativas.

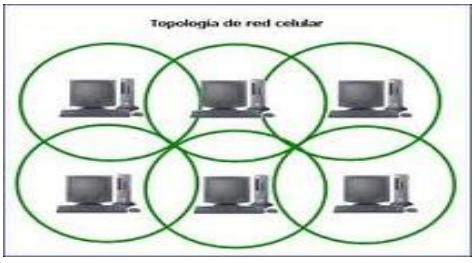
Ventajas:

- Si algún enlace deja de funcionar, la información puede ir por otro camino.

Desventajas:

- Es cara y compleja.

Red celular



Características:

- La red está compuesta por áreas circulares o hexagonales, llamadas celdas, cada una de las cuales tiene un nodo en el centro.
- Es la topología usada por las redes inalámbricas.
- En esta tecnología no existen enlaces físicos, funciona por medio de ondas electromagnéticas (radio, infrarrojos, microondas, etc...).

Ventajas:

- Eliminación de los cables.

Desventajas:

- Problemas típicos de las señales electromagnéticas.
- Problemas de seguridad.

CARACTERÍSTICAS DE LAS REDES

- Compartición de archivos
- Compartición de impresoras
- Servicios de aplicación
- Acceso remoto
- Seguridad de la red

MODELOS DE REDES

Siempre que se pretende una comunicación del tipo que sea, se deben cumplir una serie de requisitos básicos, como son el tipo de lenguaje a utilizar, el tipo de información a transmitir, el momento, el modo, etc.

Cuando dos equipos intentan establecer una comunicación deben hablar el mismo lenguaje y ponerse de acuerdo en una serie de normas. Estas normas mutuamente aceptadas van a regir el diálogo entre los equipos de una red.

Para que esta comunicación sea más sencilla de implementar se divide en niveles o capas. Así, la comunicación entre equipos queda estructurada por niveles y forma lo que se llama una arquitectura de protocolos de comunicaciones.

Modelo de Referencia OSI (Interconexión de Sistemas Abiertos)

El modelo de referencia OSI intenta crear una estructura de manera que el problema de la comunicación entre equipos pueda ser abordado del mismo modo por todas aquellas personas encargadas de desarrollar hardware y software para una red.

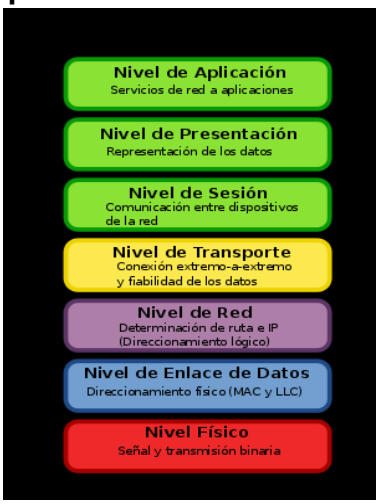
El modelo de referencia OSI es un marco teórico que no se aplica realmente en la práctica ya que existen otras arquitecturas que se desarrollaron con más rapidez y que, demostrada su validez, se han implantado de forma generalizada.

El modelo de referencia OSI es la definición de un modelo de arquitectura, desarrollado por la Organización de Estándares Internacionales (ISO, International Standar Organization). Este es frecuentemente usado para describir la estructura y función de los protocolos de comunicaciones de datos.

Este modelo llamado Interconexión de Sistemas Abiertos (OSI, Open System Interconnect), provee una referencias para todos los sistemas de comunicación.

Este modelo de referencia posee 7 capas que definen las funciones de los protocolos de comunicaciones de datos.

Capas o niveles del Modelo OSI



Cada capa del modelo OSI presenta la ejecución de una función, cuando los datos son

transferidos entre aplicaciones cooperativas que están corriendo en la red.

Características Fundamentales del Modelo OSI

En el modelo de referencia OSI se pueden distinguir tres características fundamentales:

- Arquitectura, en la cual se definen los aspectos básicos de los sistemas abiertos.
- Servicios, proporcionados por un nivel al nivel inmediatamente superior.
- Protocolos, es decir, la información de control transmitida entre los sistemas y los procedimientos necesarios para su interpretación.

Capas del Modelo OSI

Nivel Físico

Se encarga de la transmisión de bits por un medio de transmisión. Este nivel define el medio de transmisión y los conectores desde cuatro puntos de vista:

- Mecánico: tipo de cable , aislante, etc...
- Eléctrico: voltaje que representa un 1 y el que representa un 0, frecuencia, tipo de onda, velocidad de transmisión de cada bit, etc..
- Funcionales: tipo de conectores, número y uso de los pines, etc...
- De procedimiento: secuencia de eventos por la cual las cadenas de bits son intercambiadas.

Nivel de Enlace de Datos

Envía tramas de datos entre estaciones (o routers) de una misma red. Su función es conseguir que exista una transmisión fiable solventando los problemas de ruido que pueda haber en la red.

Los protocolos de este nivel son responsables de delimitar las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama.

Ofrece la transmisión y recuperación fiable de datos, con varias funciones: Control de errores (detección/corrección), delimitación o sincronización de tramas y control de flujo.
Algunos protocolos del nivel de enlace: CSMA/CD y Paso testigo.

Nivel de Red

Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los datos se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Este nivel se encarga de mandar los paquetes de información por el camino más adecuado para que llegue en el menor tiempo posible y evitando, a la vez, que las redes se lleguen a saturar.

Aparte, este nivel, se ocupa de la conexión y desconexión de redes, su sincronización, control de flujo de la información entre redes, detección de errores de transmisión y recuperación de los errores que se puedan producir, así como evitar la congestión por exceso de paquetes en alguna parte de la subred.

Nivel de Transporte

Es el corazón del modelo OSI. Ofrece mecanismos fiables para el intercambio de datos de un extremo a otro, realiza servicios de detección de errores que aseguran la integridad de los datos así como los niveles de calidad de los servicios y se encarga de la multiplexación entre aplicaciones distintas.

Las tramas de datos viajan sin orden por la red, este nivel tiene la función de recomponer la información para que tenga sentido; será el encargado de eliminar las tramas repetidas y ponerlas todas en el orden correcto.

Ejemplos de protocolos de este nivel son: TCP y UDP.

Nivel de Sesión

Proporciona funciones de organización y sincronización para que las aplicaciones dialoguen entre si. El diálogo se realiza a través del uso de una conexión que se llama sesión.

Son mecanismos complejos que consiguen determinar en que punto se encuentra exactamente una comunicación si ocurre un error fatal.

Nivel de Presentación

Se encarga de la presentación de los datos intercambiados entre entidades de nivel de aplicación, es decir, la sintaxis de estos datos.

Actúa como un traductor de manera que, cualquiera que sea la aplicación que desea emplear los servicios de la red, los datos se traducen a un formato universal.

Se ocupa de los aspectos de representación de la información, por ejemplo, se ocupa del tipo de codificación de los datos previamente establecido. También se ocupa de la compresión de los datos y de su encriptación.

Nivel de Aplicación

Este nivel enlaza directamente con el usuario real. Proporciona servicios de red a procesos de aplicacion.

Son funciones de uso común para muchas aplicaciones, (emulación de terminales, transferencia de archivos, correo electrónico...).

Modelo de Referencia TCP/IP (Familia de Protocolos TCP/IP)

La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: TCP e IP.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

Capas y Protocolos del Modelo TCP/IP

Capa de Interfaz de red

En esta capa, el software TCP/IP de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica.

Una interfaz de red puede consistir en un dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que las máquinas están conectadas directamente) o un complejo subsistema que utiliza un protocolo de enlace de datos propios.

Capa Internet

La capa Internet maneja la comunicación de una máquina a otra. Ésta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. También maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Por último, envía los mensajes de error y control necesarios.

Capa de Transporte

La principal tarea de esta capa es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto.

Esta capa regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Además divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión.

Capa de Aplicación

Es el nivel mas alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continuo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

OSI vs TCP/IP (Critica a los Modelos)

Modelo OSI

- Aparición inoportuna: Los protocolos TPC/IP ya eran utilizados en el momento en que aparecieron los protocolos OSI.
- Mala tecnología: Tanto el modelo como los protocolos tienen defectos.
- Malas implementaciones: Ya que el modelo es grande, las implementaciones eran muy complejas.

Modelo TCP/IP

- El modelo no sirve de guía para diseñar redes nuevas mediante tecnologías nuevas.
- El modelo es practicamente inexistente, pero los protocolos tienen un amplio uso.

UNIDAD II

CONECTIVIDAD DE REDES

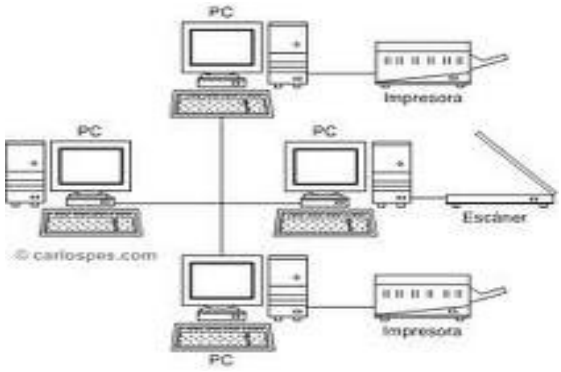
- Red de igual a igual
- Red cliente/servidor
- Puestos de trabajo en la conectividad de redes
- Protocolos de conectividad

Filosofías de Red

Las filosofias de red ó relaciones entre redes, definen la forma en que una computadora utiliza los recursos de otra computadora a través de la red.

Existen dos tipos de relaciones fundamentales entre redes: de igual a igual y cliente/servidor.

RED DE IGUAL A IGUAL



Una relación en una red de igual a igual se define como una donde las computadoras de la red se comunican entre sí al mismo nivel.

Cada computadora es responsable de poner a disposición de las otras computadoras de la red sus propios recursos.
Cada computadora también es responsable de configurar y mantener la seguridad de estos recursos.
Cada computadora es responsable de acceder a los recursos de red que ésta necesite de otras computadoras y de saber donde se encuentran dichos recursos y que seguridad se requiere para acceder a los mismos.

Ventajas:

- **Utilizan hardware de cómputo más barato:** Tienen una carga de trabajo baja ya que los recursos están distribuídos; por lo tanto, no se tiene la necesidad de una computadora que actúe como servidor.
- **Fácil de administrar:** Cada computadora lleva a cabo su propia administración, por lo tanto, el esfuerzo que se requiere para admisntrar la red se distribuye entre muchos.
- **Más redundancia integrada:** Al tener la información distribuída en la red, ante un fallo en cualquier computadora, se cuenta aún con gran parte de los recursos de la red.
- **No requieren de un sistema Operativo de Red (NOS):** Para formar una red de igual a igual basta con tener sistemas operativos de escritorios, ya que no se requiere la robustes de los sistemas operativos de red.

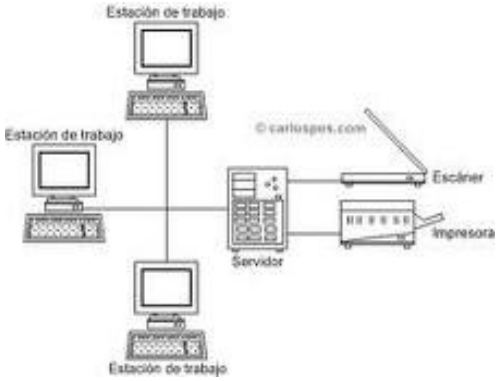
Desventajas:

- **Puede afectar el desempeño del usuario:** El hecho de que otras computadoras usen los recursos instalados en alguna computadora, puede afectar de manera negativa el rendimiento de la computadora donde están instalados los recursos.
- **No son muy seguras:** Ya que no se puede garantizar que quien utiliza las

computadoras las administre de manera adecuada.

- **Difíciles de respaldar:** El respaldo confliable de todos los datos distribuidos en varias estaciones es dificil.
- **Difícil de mantener un control de las versiones:** Con archivos almacenados en diferentes estaciones, puede ser difícil controlar las versiones de los diferentes documentos.

RED CLIENTE/SERVIDOR



Una relación de red cliente/servidor es aquella en la que se distinguen entre las computadoras que ponen a disposición los recursos de la red (los servidores) y aquéllas que utilizan los recursos (los clientes o estaciones de trabajo).

Una red cliente/servidor pura es aquella en la que todos los recursos residen y están administrados centralmente, y despues, son accesados por las computadora clientes. Estas en ningún momento comparten sus recursos a otras computadoras, en lugar de eso son exclusivamente consumidoras de estos recursos.

Las computadoras servidoras instaladas en estas redes son responsables de poner a disposición y administrar los recursos compartidos apropiados, así como de admisnitrar

la seguridad de los mismos.

Ventajas:

- **Son muy seguras:** Al estar la información y/o recursos centralizados, la administración es más fácil y segura. Al estar los servidores ubicados fisicamente en un lugar seguro bajo acceso restringido se incrementa la seguridad. Los sistemas operativos de red están diseñados para ser seguros.
- **Mejor desempeño:** Los servidores están diseñados para manejar las necesidades de múltiples usuarios de forma simultánea.
- **Respaldo centralizado:** Los respaldos son más fáciles y rápidos cuando la información se encuentra centralizada, además de que se pueden llevar a cabo en horarios de menos acceso a la información.
- **Muy confiables:** Los servidores son más confiables que las estaciones de trabajo, ya que pueden manejar fallas de disco, de procesador, de alimentación , etc.
-

Desventajas:

- **Requieren de administración profesional:** Al requerir de una administracion profesional para la red, se incrementan los gastos de administración.
- **Uso más intenso del hardware:** Los servidores deben ser equipos poderosos, lo cual implica un incremento considerable en los costos de hardware y software.

PUESTOS DE TRABAJO EN LA CONECTIVIDAD DE REDES

Administrador de red (administrador de sistemas):

Son responsables de las operaciones de la misma red, o en compañías grandes, de las

operaciones de una parte clave de la red. Sus principales tareas son:
Crear, mantener y eliminar cuentas de usuario.
Asegurar que los respaldos se hagan de manera regular.
Administrar las claves de la red.
Administrar las políticas de seguridad.
Agregar y admministrar equipo de conectividad (servidores, ruteadores, etc.)
Supervisar el hardware y software de la red.
Reparar los problemas de la red.
Las certificaciones MCSE, MCSA o CNE son importantes para un buen administrador de red.

Ingeniero de redes:

Los ingenieros están más enfocados con los bits y bytes de una red. Es típico que tengan un grado académico en ingeniería y se espera que sean expertos en los sistemas operativos de red con los que trabajan y, en especial, en elementos clave del hardware de la red, como dispositivos de interconexión.
También son el personal que repara, diagnostica y soluciona los problemas que superan la capacidad del administrador de la red.
Los ingenieros poseen años de experiencia en operación y reparación de redes complejas. Asimismo, tiene certificaciones de las compañias que fabrican equipo de conectividad de redes, como el programa de certificación de Cisco.

Arquitecto/diseñador de red:

Los diseñadores de red trabjan, en general, para compañías que venden y dan soporte a redes o para grandes empresas que tienen redes enormes que están en constante cambio y expansión. En escencia, diseñan redes.
Deben comprender las necesidades del negocio que la red necesita satisfacer, así como conocer a fondo los productos de conectividad de redes disponibles en el

mercado y la forma en que éstos interactúan.

También son importantes cuando se necesita expandir una red compleja y ayudan a asegurar que las nuevas adiciones no provoquen problemas.

Administrador de la base de datos:

El administrador de base de datos es la persona responsable de los aspectos ambientales de una base de datos. En general esto incluye lo siguiente:

Recuperabilidad: Crear y probar respaldos.

Integridad: Verificar o ayudar a la verificación en la integridad de datos.

Seguridad: Definir o implementar controles de acceso a los datos.

Disponibilidad: Asegurarse del mayor tiempo de encendido.

Desempeño: Asegurarse del máximo desempeño.

Desarrollo y soporte a pruebas: Ayudar a los programadores e ingenieros a utilizar eficientemente la base de datos.

El diseño lógico y físico de las bases de datos.

PROTOCOLOS DE CONECTIVIDAD

Protocolo ARP (Protocolo de Resolución de Direcciones)

El protocolo ARP permite obtener una dirección física (dirección MAC) de un dispositivo, dada su dirección lógica (dirección IP).

Este protocolo se encuentra en el nivel de Host a red (Red) del Modelo TCP/IP.

Cada vez que una computadora o un enrutador tiene un datagrama IP para enviar a otra computadora o enrutador, incluye la dirección lógica del receptor. Pero el datagrama IP debe ser encapsulado en una trama para que pueda pasar a través de la red fisica. Esto implica que el emisor necesita conocer la dirección física del receptor.

Funcionamiento:

Los pasos involucrados en un proceso ARP son:

1. El emisor sabe la dirección IP del destino.
2. IP pide a ARP que cree un mensaje de consulta ARP, rellenando la dirección física del emisor, la dirección IP del emisor y la dirección IP destino. El campo de dirección física del destino se rellena con ceros.
3. El mensaje se pasa al nivel de enlace donde es encapsulado en una trama usando la dirección fisica del emisor, dirección origen y la dirección fisica de broadcast como dirección destino.
4 . Cada computadora o enrutador recibe la trama ya que es un mensaje de broadcast. Cada estación lo pasa a su ARP. Todas las máquinas excepto la destino descartan el paquete. La máquina destino reconoce su dirección IP.
5. La maquina destino responde con un mensaje de respuesta ARP que contiene su dirección física. Este mensaje es unicast.
6. El emisor recibe el mensaje de respuesta. Ahora conoce la dirección física del destino.
7. El datagrama IP, que lleva los datos del destino, es encapsulado ahora en una trama y enviado al destino.

Protocolo RARP (Protocolo de Resolución de Direcciones Inverso)

El protocolo RARP permite hallar la dirección lógica para una máquina que sólo conoce su dirección física.

Este protocolo se encuentra en el nivel de Host a red (Red) del Modelo TCP/IP.

En algunas ocasiones una computadora conoce su dirección física, pero necesita conocer su dirección lógica.

Esto puede ocurrir cuando en una organización no se tienen suficientes direcciones IP para asignar a cada estación; por lo que se asignan bajo demanda.

La estación puede enviar su dirección física y pedir una dirección IP dedicada para un

periodo de tiempo.

Funcionamiento:

Para crear un datagrama IP, una computadora necesita conocer su propia dirección IP. Cuando una máquina no puede obtener su direccion IP directamente realiza lo siguiente:

1. La máquina obtiene su dirección fisica (leyendo su NIC).
2. Crea una petición RARP y se envía a la red local.
3. El servidor RARP responde con un mensaje RARP. Enviandole una dirección IP disponible.

Hay un serio problema con RARP, el broadcast se hace a nivel de enlace. La dirección fisica de broadcast, no pasa las fronteras de una red. Esto significa que si un administrador tiene varias redes, necesita asignar un servidor RARP para cada una. Esta es la razón de que RARP esté casi obsoleto.

Protocolo DHCP (Protocolo de Configuración de Host Dinámico)

El protocolo DHCP esta diseñado para proporcionar una asociación de dirección física a dirección lógica.

Este protocolo proporciona asignación estática y dinámica de direcciones.

DHCPDISCOVER: Es el primer paso en el proceso de concesión de DHCP. Para comenzar el proceso un cliente difunde un mensaje DHCPDISCOVER que solicita la localización de un servidor de DHCP y de la información de dirección IP. Este mensaje contiene la siguiente información:

Dirección MAC del cliente.

Nombre del equipo.

DHCPOFFER: En este segundo paso, todos los servidores de DHCP que reciban la petición de concesión de IP, difunden un mensaje DHCPOFFER con la siguiente información:

Dirección MAC cliente.

Dirección IP ofrecida.

Longitud de la concesión.

Identificador del servidor.

DHCPREQUEST: Después de que el cliente recibe un DHCPOFFER de al menos un servidor de DHCP y selecciona una dirección IP. El cliente difunde un mensaje DHCPREQUEST a todos los servidores de DHCP, indicando que ha aceptado una

oferta. Este mensaje incluye:
Dirección IP del servidor cuya oferta se acepta.

DHCPACK: El paso final en un DHCP ocurre cuando el servidor de DHCP que emite la oferta aceptada difunde un reconocimeinto afirmativo al clliente en la forma de mensaje DHCPACK. Este mensaje contiene una concesión válida para una dirección IP.
Cuando el cliente de DHCP recibe el reconocimiento, se inicia totalmente TCP/IP y el cliente se considera ligado para comunicarse en la red.

DHCRELEASE: Cuando un cliente de DHCP quiere liberar la concesión, envía un mensaje DHCPRELEASE al servidor de DHCP para que libere la concesión.

Asignación de direcciones dinámica: DHCP tiene una base de datos que asocia etáticamente direcciones físicas a direcciones IP.
DHCP tiene una segunda base de datos con un conjunto de direcciones IP disponibles. Cuando un cliente DHCP pide una dirección temporal IP, el servidor DHCP consulta el conjunto de direcciones IP disponibles y asigna una dirección IP durante un peirodo de tiempo.

Cuando un cliente DCHP envía una petición a un servidor DHCP, el servidor comprueba primero su base de datos estática. Si existe una entrada con la dirección física del cliente en la base de datos estática, se devuelve la dirección IP permanente del cliente.

Por otro lado, si la entrada no existe en la base de datos estática, el servidor selecciona una dirección IP del conjunto disponible, asigna la dirección al cliente y añade la entrada en la base de datos dinámica.

Las direcciones asignadas del conjunto disponible son direcciones temporales. El servidor DHCP emite un contrato de arrendamiento durante un tiempo específico. Cuando el contrato expira, el cliente debe dejar de usar la dirección IP o renovar el contrato. El protocolo DHCP es un protocolo de la capa de Aplicación.

Protocolo ICMP (Protocolo de Control de Mensajes de Internet)

El protocolo ICMP es el protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

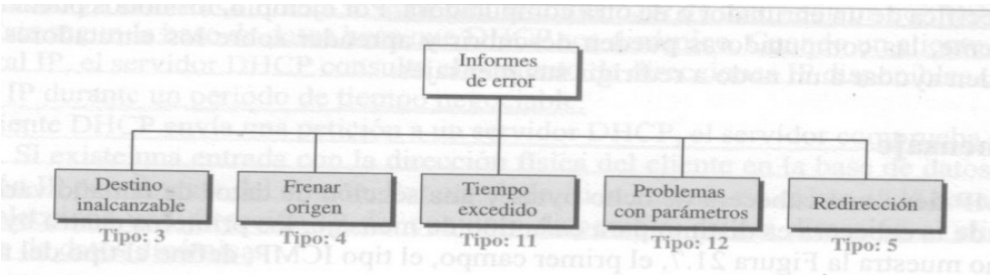
Tipos de mensajes:

Los mensajes ICMP se dividen en dos categorías:

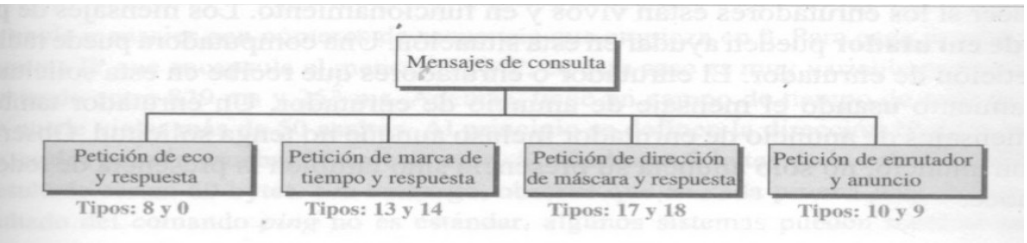
Mensajes de informe error: Estos mensajes informan de problemas que un enrutador o una computadora puede encontrar cuando procesa un paquete IP.

Mensajes de consulta: Estos mensajes ayudan a una computadora o gestor de red a tener información específica de un enrutador o de otra computadora.

Tipos de mensajes de informe de error:



Tipos de mensajes de consulta:



ICMP no corrige errores, solamente informa de ellos. Los mensajes de error siempre se envían al origen de la transmisión. Además de informar de los errores, ICMP puede diagnosticar algunos problemas en la red. Esto se lleva a cabo mediante los mensajes de consulta. El protocolo ICMP es un protocolo de la capa de Host a red (Red).

Protocolo IP (Protocolo de Internet)

Este protocolo, funciona transmitiendo la información por medio de paquetes de datos llamados **datagramas**, desde el origen al destino.

Para hacer esto, identifica a los host origen y destino por una dirección de longitud fija, llamada **dirección IP**.

Se encarga de la fragmentación y reensamblaje de grandes datagramas para su transmisión por redes de trama pequeña.

Es un protocolo que pertenece a la capa de Internet (Red).

Es un protocolo *de* conmutación de paquetes no orientado a conexión, ya que cada paquete viaja independientemente de los demás.

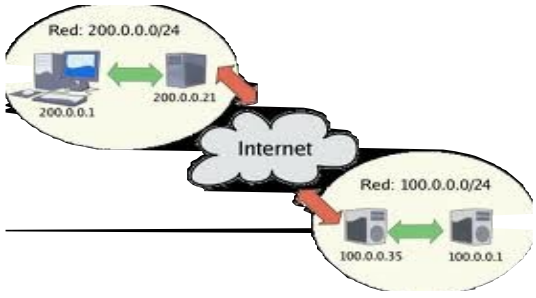
Es un protocolo no fiable, los paquetes se pueden perder, duplicar o cambiar de orden. Es decir este protocolo no soluciona estos problemas, esta tarea queda para otros protocolos.

El protocolo IP realiza dos funciones básicas: **direccionamiento y fragmentación**:

Cada datagrama IP tiene una cabecera en la que figuran la dirección de origen y de destino. El módulo internet usa estas direcciones para llevar el datagrama hasta su destino. Este proceso se llama *encaminamiento o enrutamiento*.

El módulo Internet usa campos en la cabecera para fragmentar y reensambla los datagramas IP, si fuera necesario, para su transmisión por redes de trama pequeña.

Funcionamiento:



Dos hosts que se encuentran en dos redes distintas unidas por una pasarela y quieren intercambiar información. Su modo de operación es el siguiente:

El origen prepara sus datos y llama a su módulo internet local, que se encargará de enviar esos datos como datagramas IP, para ello, prepara la cabecera del datagrama y

adjunta los datos a él con la dirección de destino y otros parámetros como argumentos de la llamada.

El módulo Internet decide, por la dirección IP del destino, que debe enviarlo a otra red local. El datagrama llega a la pasarela encapsulado. Esta pasarela, a su vez llama a su módulo internet. Este, comprueba si el datagrama debe ser reenviado a otro host en una segunda red. Así sucesivamente, hasta llegar a la red local a la que pertenece el host de destino.

El host destino, a su vez, llama a su módulo internet, pasando la dirección de origen y otros parámetros como resultado de la llamada.

Todo este proceso se basa en la interpretación de una dirección internet. Por eso, un importante mecanismo del protocolo IP es la **dirección internet.**
En su ruta, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad, el protocolo IP proporciona un mecanismo de fragmentación.

Direccionamiento:
El protocolo IP maneja únicamente direcciones, la dirección Internet.
Cuando se quiere enviar un mensaje a través de un sistema de redes no se puede emplear la dirección física de la tarjeta ya que no existe un modo estandarizado de identificar un host dentro de una red, dentro de un sistema de múltiples redes, que sea efectivo. Así, se ha ideado la dirección IP, que permite identificar la red en la que se encuentra la computadora y, a la vez, ubicar la posición de ésta PC dentro de la red.

Para poder identificar una máquina en Internet cada una de ellas tiene una **dirección IP** (Internet Protocol) la cual es asignada por **IANA**, organismo internacional encargado

de asignar las direcciones IP públicas, aunque se dedica a asignar las direcciones de red de las empresas y estas ya se encargan de administrar sus equipos.

El sistema de direccionamiento IP consiste en una serie de dígitos. Se representa con cuatro campos separados por puntos, como 193.144.238.1, no pudiendo superar ninguno de ellos el valor 255 (11111111 en binario).

Protocolo IP

Estas direcciones numéricas son las que entiende la máquina y se representan por 32 bits con 4 campos de 8 bits cada uno, aunque normalmente se pasan de binario a decimal.

Por ejemplo 139.3.2.8 es en numeración binaria:
10001011 00000011 00000010 00001000 Binario
139. 3. 2. 8 Decimal

Cualquier dirección IP de un host tiene dos partes, por un lado, aquella que identifica la red a la que pertenece la computadora y por otro, la computadora dentro de la red en la que se encuentra.

Para determinar qué parte de la dirección de Internet se refiere a la red y cuál pertenece a la computadora se debe introducir la máscara de subred que permite identificar los dígitos de la dirección IP que pertenecen a cada una de sus partes.

Si la dirección IP se compone de cuatro grupos de ocho bits, se crea una máscara en la que, de alguna forma se indica cuáles de esos bits pertenecen a la red y cuales al host. Los dígitos de valor uno de la máscara de subred indican la parte de la dirección IP que identifica la red, y los de valor cero, indican a la computadora. Así, la dirección

IP de un equipo siempre debe estar asociada a una máscara de subred.

Ejemplo:

Máscara de subred

11111111 11111111 11111111 00000000

Dirección IP

11000000 10101000 00000000 10101100

Significado

Red Host

Clases de direcciones IP:

CLASE	DIRECCIONES DISPONIBLES: DESDE	HASTA	CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
A	0.0.0.0	127.255.255.255	126*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.x.x.x está reserevado como dirección de loopback para pruebas y diagnóstico

Existen cinco clases de direcciones IP según la manera de repartir los bits entre la dirección de red y el número de host.

Protocolo TCP (Protocolo de Control de Transmisión)

Protocolo de control de transmisión de la capa de transporte, que regula las cuestiones relativas al transporte de la información.

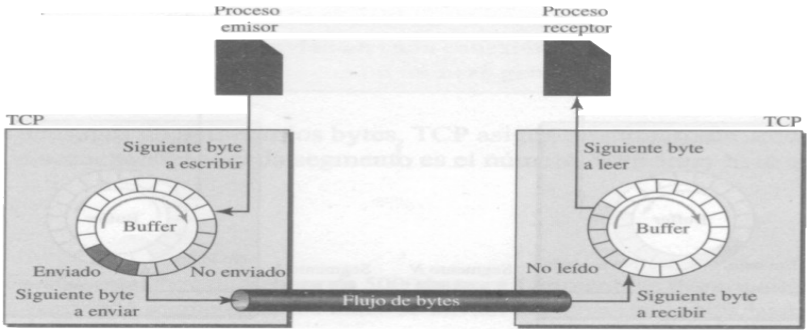
El protocolo TCP se encarga de regular el flujo de la información, de tal forma que éste se produzca sin errores y de una forma eficiente. Proporciona calidad de servicio.
El protocolo TCP es un protocolo de la capa de Transporte.

TCP es un protocolo:
Orientado a la conexión: esto significa que se establece una *conexión* entre emisor y receptor, previamente al envío de los datos. Se establece un *circuito virtual* entre los extremos. Este circuito crea la ilusión, por esto se llama virtual, de que hay un único circuito por el que viaja la información de forma ordenada.
Esto, en realidad no es cierto, la información viaja en paquetes desordenados por distintas vías hasta su destino y allí, tiene que ser reensamblada.

Fiable: significa que la información llega *sin errores* al destino. Por esto, la aplicación que usa este protocolo, no se tiene que preocupar de la integridad de la información, se da por hecho.
El protocolo **TCP** actúa de puente entre la aplicación, que requiere sus servicios, y el **protocolo IP**, que debe dirigir el tráfico por la red, hasta llegar a su destino. Los datos viajan en paquetes de información llamados **segmentos**.

Funcionamiento:
Para poder enviar información, es necesario establecer una conexión entre los extremos. En una transmisión hay tres fases:
1. Apertura de conexión.
2. Transferencia de datos.
3. Cierre de conexión.

Envío de segmentos TCP:



Apertura de conexión:

Para abrir la conexión se envían tres segmentos, por eso se llama *"saludo de tres vías"*:

1. La computadora 1(O1), hace una *apertura activa* y envía un segmento TCP (S1), a la computadora 2 (O2).
2. O2 recibe el segmento (S1). Si desea abrir la conexión, responde con un segmento (S2) acuse de recibo (ACK), y deja abierta la conexión.
3. O1 recibe el segmento (S2) y envía su segmento (S3) de confirmación.
4. O2 recibe la confirmación (S3) y decide que *la conexión ha quedado abierta.* Aqui comienza la transmisión de datos.

Transferencia de datos:

Para controlar el flujo de la transmisión, el protocolo TCP, usa unas técnicas conocidas con el nombre de *"Solicitud de Repetición Automática"* (ARQ*)*, mediante el cual el receptor (O2) envía un mensaje de acuse de recibo (ACK), cada vez que recibe un segmento TCP del emisor (O1).

Para controlar la transmisión, TCP numera los segmentos secuencialmente. En el receptor, TCP reensambla los segmentos como estaban en el inicio. Si falta algún número de secuencia en la serie, se vuelve a transmitir el segmento con ese número.
Durante la transmisión se pueden presentar errores, hay varias técnicas para detectar y corregir los posibles errores en la transmisión.

Las más usadas son las siguientes:

- Comprobación de la paridad.
- Suma de chequeo (checksum).
- Comprobación de la redundancia cíclica (CRC).

Cierre de la conexión:

Cuando el origen ya no tiene mas datos para transferir. Envia un segmento TCP indicando al destino que desea cerrar la conexion activa.
El destino informa a su aplicacion del cierre de la conexion y envia un segmento TCP de confirmación al origen.
El origen recibe la confirmación. El destino envia un segmento TCP para finalizar.
El origen recibe el segmento TCP de finalizar, envia un segmento TCP al destino de finalizar y cierra su conexión, el destino recibe el mensaje y cierra su conexión.

Protocolo UDP (Protocolo de Datagrama de Usuario)

Este protocolo proporciona una comunicación sencilla entre dos computadoras, y no consume muchos recursos.
Es un protocolo que pertenece a la capa de transporte.
No confiable: no hay un control de paquetes enviados y recibidos. Estos pueden llegar erróneos o no llegar a su destino.

No orientado a conexión: no se realiza una conexión previa entre origen y destino, como ocurre en el protocolo TCP.

Es un protocolo útil, en casos en los que no es necesario mucho control de los datos enviados. Se usa cuando la rapidez es más importante que la calidad. No es tan fiable pero es simple, con baja sobrecarga de la red, y por lo tanto ideal para aplicaciones que usen masivamente la red.

Utiliza el protocolo IP para transportar los mensajes, es decir, va encapsulado dentro de un datagrama IP.

No controla errores, cuando se detecta un error en un datagrama, se descarta.

UDP no numera los datagramas, tampoco utiliza confirmación de entrega, Esto hace que no hay garantía de que un paquete llegue a su destino, ni

que los datagramas pueden llegar duplicados o desordenados a su destino.

Algunas situaciones en las que es más útil el protocolo UDP, son:

Aplicaciones en *tiempo real* como audio o video, donde no se admiten retardos.

Consultas a servidores en las que se envían uno o dos mensajes solamente, como es el caso del DNS.

En transmisiones en modo multicast (a muchos destinos), o en modo broadcast (a todos los destinos), ya que si todos los destinos enviaran confirmación el emisor se colapsaría.

Protocolo HTTP (Protocolo de Transferencia de Hipertexto)

Es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores http.

Se diseñó específicamente para el World Wide Web: es un protocolo rápido y sencillo que permite la transferencia de múltiples tipos de información de forma eficiente y rápida.

Cada vez que un cliente realiza una petición a un servidor, se ejecutan los siguientes pasos:

1. Un usuario accede a una URL, seleccionando un enlace de un documento HTML o introduciéndola en el navegador.
2. El cliente Web descodifica la URL, separando sus diferentes partes. Así identifica el protocolo de acceso, la dirección DNS o IP del servidor y el objeto requerido del servidor.
3. Se abre una conexión TCP con el servidor web, llamando al puerto TCP correspondiente (80).
4. Se realiza la petición.
5. El servidor devuelve la respuesta al cliente.
6. Se cierra la conexión TCP.

Este proceso se repite en cada acceso al servidor HTTP.

Protocolo FTP (Protocolo de Transmisión de Archivos)

El Protocolo de Transmisión de Archivos es usado para “subir” o “bajar” archivos entre una estación de trabajo y un servidor FTP.

Existen en la red Internet cientos de computadoras que son servidores de archivos de acceso público, existen programas clientes que permiten hacer FTP de una manera sencilla y completa. Aunque también se puede utilizar el propio Navegador.

Para hacer FTP con el navegador se tiene que poner en la barra de direcciones "ftp://" seguido de la dirección del servidor al que se quiere acceder.

Existen dos maneras de realizar FTP con un programa cliente: FTP anónimo y FTP identificado.

Los datos principales que se requieren incluir son:

Profile Name: nombre cualquiera que sirva para identificar la conexión.

Host Name/Address: Dirección del servidor con el que se desea conectar.

User ID y Password: Estos campos se rellenan automáticamente al marcar la casilla Anonymous situada a la derecha del campo User ID. O se llena el login del usuario y su password para el caso identificado.

Protocolo DNS (Servidor de Nombres de Dominio)

Básicamente es un conjunto de software y protocolos que traducen los nombres de dominio como www.fcca.umich.mx en una dirección IP del tipo 195.53.133.44.

El Proceso de trabajo para conseguir esta dirección IP es el siguiente:

Primero el servidor de nombres verifica sus tablas de máquinas a ver si allí consigue el nombre por el cual le están preguntando. Si es así, entonces retorna la dirección IP asociada con ese nombre. Si la información pertenece a otro dominio, entonces el servidor de nombres busca en su cache y si no está allí comienza un proceso que se puede comportar de estas dos formas:

De manera Recursiva:

Un servidor de nombres envía una respuesta recursiva cuando es el servidor y no el cliente el que pregunta a otros servidores de nombres por la información del dominio solicitada. Esto ocurre cuando el servidor de nombres sabe que el *resolver* no tiene la inteligencia de manejar una referencia a otro servidor de nombres. A medida que un servidor de nombres pregunta (obtenga respuesta o no) va guardando los nombres encontrados en su cache para evitarse búsquedas innecesarias.

De manera Iterativa:

El servidor de nombres da la mejor respuesta, es decir, da una referencia al servidor de nombres más cercano a la información de dominio interrogado.

Primero consulta sus datos locales, si no está allí busca entonces en su cache y si aún no encuentra nada entonces devuelve la respuesta lo más cercano al dominio buscado.

La dirección completa de la máquina se lee de izquierda a derecha (Desde lo más específico, el nombre del host, pasando por cada uno de los "dominios" a los cuales pertenecen).

Los dominios más usuales son los siguientes: com, edu, net, org, mx, fr

UNIDAD III

COMPONENTES DE HARDWARE DE LA RED

Es importante conocer los dispositivos que permiten que las redes funcionen adecuadamente. La comprensión de estos dispositivos ayudan a planear una red, así como realizar su reparación y mantenimiento.

Componentes de hardware de la Red

- Servidores
- Computadoras clientes
- Cableado
- Dispositivos de interconexión

SERVIDORES

Un servidor es cualquier computadora que lleva a cabo funciones de red para otras computadoras. Estas funciones se clasifican en: servidores de archivo e impresión, de aplicaciones, de web y más.

Los servidores necesitan ser más confiables y serviciales que las estaciones de trabajo. Además deben hacer su trabajo de forma diferente a éstas. Por tal motivo, el hardware del servidor de la red es diferente al de una estación de trabajo.

Procesadores de Servidor:

Una gran parte del desempeño de un servidor se basa en su unidad central de proceso o CPU, el procesador es muy importante para determinar la velocidad del servidor. Los servidores pueden operar mediante el empleo de uno o muchos procesadores.

El número de procesadores que deberá tener un servidor depende de algunos factores

como son:

- El NOS a utilizar.
- El trabajo que realizará el servidor.
- Las aplicaciones que correrá el servidor.

Bus del Sistema:

Un bus es la “espina dorsal” de la transferencia de datos de un sistema de cómputo, al que se conectan el procesador, la memoria y todos los demás dispositivos instalados. Una computadora depende de su bus para mover los datos de un componente a otro. Por tanto, el bus debe ser mucho más rápido que cualquier otro componente del sistema.

Ram (Memoria de Acceso Aleatorio):

Los servidores dependen de gran medida de su capacidad de almacenar datos para lograr el mejor desempeño. Para llevar a cabo esta tarea, dependen en gran medida de su Memoria de Acceso Aleatorio (RAM).

La memoria RAM se presenta en tres variedades:

Sin paridad

Con paridad

Con verificación y corrección de errores (ECC)

Controladores de Disco:

Los datos almacenados en un servidor son, en general, de importancia crítica para la compañia, por lo que es importante tener la configuración de disco más confiable posible.

Las intefaces de disco de mayor uso son:

SATA (Conexión Serial de Tecnología Avanzada)

SCSI (Interfase para Sistemas de Cómputo pequeños)
Existen muchas variedades de sistemas de disco basadas en SCSI:
SCSI-2
Fast-SCSI
Ultra-SCSI
Ultra640 SCSI

Topologías de Disco: RAID

RAID (Arreglo Redundante de Discos Baratos) es una técnica que consiste en utilizar muchos discos para hacer el trabajo de un solo disco.

La idea fundamental de RAID radica en redistribuir los datos del servidor en muchos discos, de manera transparente, el beneficio que se obtiene es que los múltiples discos hacen el trabajo más rápido que uno solo.

Existen muchas maneras de utilizar múltiples discos. Por tanto, se definen varios niveles RAID:
RAID 0: Los datos se dividen en múltiples discos, pero sin redundancia.
RAID 1: Espejo. Los datos se respaldan en otro disco de manera sincronizada.

Componentes intercambiables:

Los componentes intercambiables son aquellos dispositivos que se pueden reemplazar mientras el sistema está en funcionamiento. En general, estos se limitan a los discos, fuentes de alimentación y ventiladores.

Supervisión del estado del servidor:

Una característica importante de los servidores es la capacidad de supervisar sus propios componentes internos y notificar si se está desarrollando algún problema.

Por lo general supervisan lo siguiente: voltaje del sistema, funcionamiento del ventilador, errores de disco, etc.

COMPUTADORAS CLIENTES

Estas máquinas son la interfase principal de los usuarios a la red y es el recurso del que dependen más los usuarios para realizar sus trabajos. En realidad, la red esta diseñada para facilitar el trabajo de las computadoras clientes, y no lo contrario. Algunos factores a tomar en cuenta cuando se eligen las computadoras clientes son:

Plataformas de escritorio

Confiabilidad y servicio

Precio y desempeño

Plataformas de Escritorio:

PC, Macintosh, Unix, linux.

Es recomendable mantener una sola plataforma en las computadoras clientes como estándar, debido a lo siguiente:

Si se elige más de una plataforma, es necesario poseer experiencia en dos plataformas, así como en sus aplicaciones.

Se requiere mayor existencia de hardware, en general, los componentes que trabajan con una PC no funcionan correctamente con una Mac y viceversa.

Proporcionar soporte a dos plataformas en más complejo que hacerlo a solo una.

Se presenta el problema de la falta de compatibilidad entre plataformas. Esto provoca problemas a los usuarios que desean trabajar juntos con diferentes plataformas.

Confiabilidad y servicio:

La confiabilidad proviene de tres fuentes:

Que la computadora use componentes probados de alta calidad.

Que dichos componentes esten diseñados para trabajar en conjunto.

El sofware que usen este certificado.
El servicio se presenta en los siguientes casos:
Tratar de que sean del mismo modelo y configuración.
Que el fabricante ofrezca software de actualización.
Amplia grantia en los equipos.

Precio y desempeño:

Es necesario tomar en cuenta la vida útil que se planee para las computadoras clientes y asegurarse de comprar sistemas que sean productivos a lo largo de su vida útil. Para esto, es necesario determinar las necesidades de cómputo que se requieren y buscar aquellos equipos que mejor las satisfagan a un precio razonable.

CABLEADO ESTRUCTURADO

El Cableado Estructurado es el cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios.

El objetivo fundamental es cubrir las necesidades de los usuarios durante la vida útil del edificio sin necesidad de realizar más tendido de cables.
En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central, facilitando la interconexión y la administración del sistema, esta disposición permite la comunicación virtualmente con cualquier dispositivo, en cualquier lugar y en cualquier momento**.**

El Cableado Estructurado trata de especificar una “Estructura” o “Sistema” de cableado

para empresas y edificios que sea:

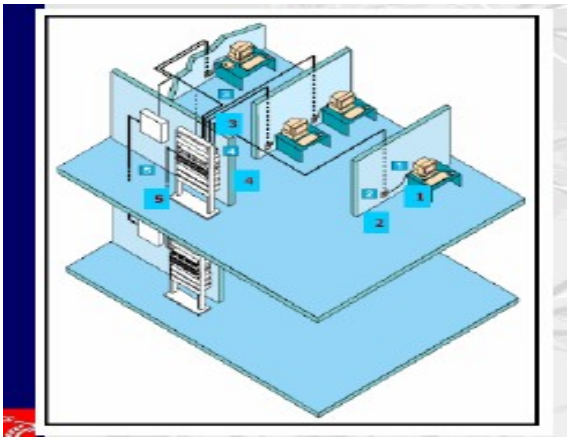
- Común y a la vez independiente de las aplicaciones
- Documentada (Identificación adecuada)
- Proyectada a largo plazo (> 10 años)

Estructura del Cableado Estructurado

- Cableado de campus: Cableado de todos los distribuidores de edificios al distribuidor de campus.
- Cableado Vertical:Cableado de los distribuidores del piso al distribuidor del edificio.
- Cableado Horizontal:Cableado desde el distribuidor de piso a los puestos de usuario.
- Cableado de Usuario:Cableado del puesto de usuario a los equipos.

Componentes del Cableado Estructurado

1. Área de trabajo
2. Toma de equipos
3. Cableado Horizontal
4. Sala de equipos (racks, closet)
5. Cableado vertical



Área de Trabajo

Los componentes del área de trabajo se extienden desde la terminación del cableado horizontal en la salida de información, hasta el equipo donde se esta corriendo una aplicación.

El cableado del área de trabajo puede variar en su forma dependiendo de la aplicación.

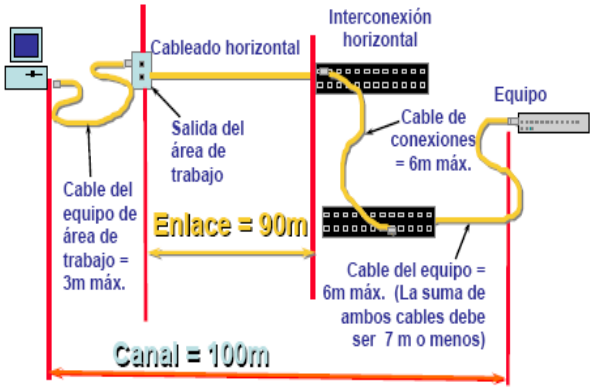
Toma de Equipos

La longitud máxima del patch cordon es de 3 metros.

Cableado Horizontal

Se extiende desde el área de trabajo hasta el armario del cuarto de telecomunicaciones. El término “horizontal” se emplea ya que típicamente el cable en esta parte del cableado se instala horizontalmente a lo largo del piso o techo falso.

Se utiliza una topología tipo estrella. Todos los nodos o estaciones de trabajo se conectan con cable UTP o fibra óptica hacia un concentrador (patch panel) ubicado en el armario de telecomunicaciones de cada piso.



Sala de Equipos

Se define como el espacio donde residen los equipos de telecomunicaciones comunes de un edificio (Servidores, racks, etc). El tamaño mínimo recomendado es 13.5 m2.

Patch Panels: Son utilizados en la terminación de cualquier tipo de cable. Son molduras de dos caras: en la cara posterior se realiza la terminación mecánica de cable y en la cara anterior se encuentran los diferentes tipos de conectores utilizados para realizar las conexiones cruzadas y se los conoce como puertos.

Cableado Verical:

Interconexión entre los armarios de telecomunicaciones, cuarto de equipos y entrada de servicios.

DISPOSITIVOS DE INTERCONEXIÓN

Los dispositivos de interconexión son responsables de la transferencia de datos de un cable de la red a otro. Cada dispositivo tiene propiedades y usos diferentes, por lo que un buen diseño de red utiliza el dispositivo correcto para cada tarea que la red debe cumplir.

Se debe conectar los diferentes dispositivos de la red en una configuración que permita que la red transfiera las señales entre los edificios de una manera lo más eficiente posible, tomando en cuenta el tipo de red y los diferentes requerimientos de conectividad de ella, se puede hacer uso de los dispositivos básicos de interconexión como son los siguientes:

Repetidores

El repetidor es un elemento que permite la conexión de dos tramos de red, teniendo como función principal regenerar eléctricamente la señal, para permitir alcanzar distancias mayores manteniendo el mismo nivel de la señal a lo largo de la red. Operan en la capa física del modelo OSI, por lo que no poseen la inteligencia para comprender las señales que transmiten.

Los repetidores solo amplifican la señal, pero tambien amplifican cualquier ruido que se produzca en el cable. Los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Debido a esto existen más riesgos de colisión y más posibilidades de congestión de la red.

Se utilizan para conectar solamente el mismo tipo de medio de transmisión.

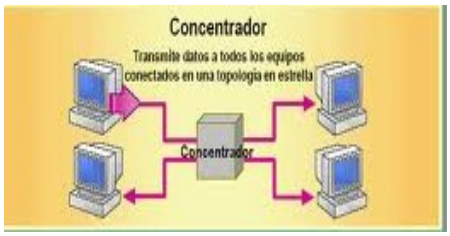
Ventajas:

- Incrementa la distancia cubierta por la LAN.
- Retransmite los datos sin retardos.
- Es transparente a los niveles superiores al físico.

Desventajas:

- Incrementa la carga en los segmentos que interconecta.

Hubs/Concentradores



Los concentradores se utilizan para conectar los nodos de red a un único dispositivo. Los nodos se conectan a los hubs fisicamente en forma de estrella. Se encuentran disponibles para cualquier tipo de medio de transmisión, así como una gran variedad de tamaños (números de puertos). Trabajan en la capa fisica del modelo OSI.

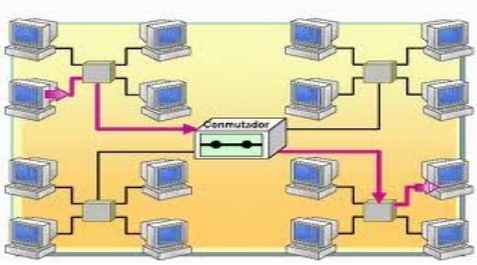
Los hubs tienen dos propiedades importantes:

- La primera propiedad: repiten todos los datos de cada puerto a todos los demas puertos. Debido a esto no se presenta ningun filtrado para evitar las colisiones.
- La segundad propiedad: es la partición automática, donde el hub puede automaticamente cortar cualquier nodo que tenga problemas.

Algunas propiedades avanzadas que soportan algunos hubs son:

- Admimistración integrada.
- Autodetección de diferentes velocidades.
- Enlaces de alta velocidad, que conectan el hub a la espina dorsal.

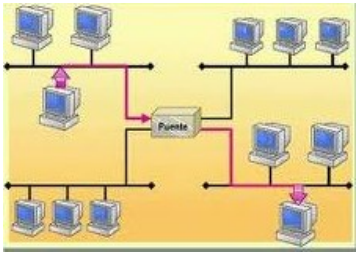
Switches

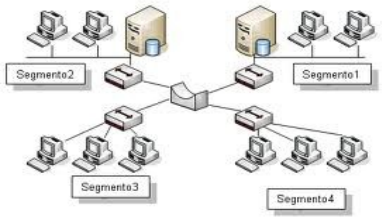


Los switches al igual que un hub permite conectar los nodos de una red, pero los switches pueden conmutar conexiones de un puerto a otro.
Tienen la funcionalidad de los hubs a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto es posible debido a que los equipos configuran unas tablas de encaminamiento con las direcciones MAC asociadas a cada uno de sus puertos.

La mayoria de las redes actuales evitan los hubs a favor de un diseño basado en switches. Trabaja en la capa de enlace de datos del modelo OSI.

Puentes





Los puentes pueden conectar dos segmentos de red entre sí, pero tienen la inteligencia suficiente para envíar tráfico de un segmento a otro soló cuando el tráfico está destinado para ese otro segmento.
Los puentes se usan para segmentar redes en tramos más pequeños. Trabajan en la capa de enlace de datos del modelo OSI.

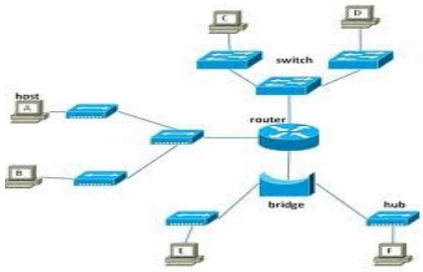
Los puentes analizan la dirección de control de acceso al medio de cada paquete que encuentran, a fin de determinar si deben enviar dicho paquete a otra red.
Las redes conectadas a través de puentes aparentan ser una única red, ya que realizan su función transparentemente.

Un puente ejecuta tres tareas básicas:

- Aprendizaje de las direcciones de nodos en cada red.
- Filtrado de las tramas destinadas a la red local.
- Envío de las tramas destinadas a la red remota.

Se deben de utilizar en redes pequeñas o en lugar de un repetidor. Como mejor opción se debe usar un router.

Ruteadores

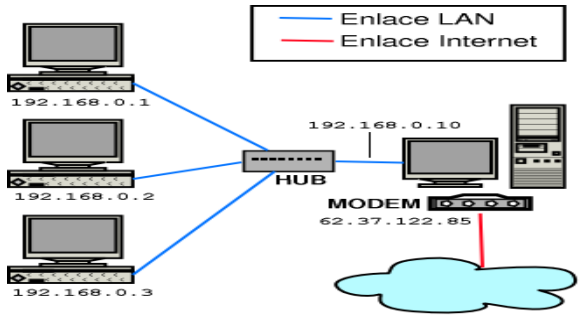


Son dispositivos inteligentes que envían paquetes de datos desde una red a otra. Los ruteadores pueden conectar tanto redes similares como diferentes. Tienen su propia dirección de red, por lo que, otros nodos envían paquetes al ruteador, que analiza el contenido de los paquetes y los transfiere a donde corresponda.

Tambien pueden determinar y usar la ruta más corta para alcanzar un destino. Se ajustan en forma dinámica a los problemas cambiantes o patrones de tráfico de una red. Los ruteadores funcionan en la capa de red del modelo OSI.

Deben programarse para funcionar de manera correcta, deben tener las direcciones asignadas a cada uno de sus puertos. Se utilizan en los enlaces de la redes de área amplia. (WAN).

Compuertas/Gateway/Puerta de enlace



Son interfaces de aplicación específica que enlazan las siete capas del modelo OSI cuando son diferentes en uno o todos los niveles. Permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito

es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Debido a que los gateway tienen que realizar muchas traducciones, tienden a ser más lentas que otras soluciones.
El uso principal de estos dispositivos es concetar una red local a una red exterior.

Firewalls/Cortafuegos

Es un dispositivo que se instala entre dos redes y refuerza las politicas de seguridad.
En general un firewall se coloca entre la LAN de una compañia e Internet , pero tambien puede colocarse entre una LAN y WAN.

Existen básicamente dos diferentes tipos de firewalls:

- Basados en red: Trabajan a nivel de red, como filtrado de paquetes IP.
- Basados en aplicación: Los filtrados se adaptan a las caracteristicas propias de cada protocolo. Por ejemplo, si se trata de trafico HTTP, se realiza filtrado según la URL.

UNIDAD IV

SISTEMAS OPERATIVOS DE RED

- Introducción a los sistemas operativos de red
- Servicios de directorio
- Cuentas de usuario y de grupo
- Sistemas de archivos y unidades
- Servicios de red

INTRODUCCIÓN A LOS SISTEMAS OPERATIVOS DE RED

Definición de Sistema Operativo de Red

Es un componente software de una computadora que tiene como objetivo coordinar y manejar las actividades de los recursos de la computadora en una red de equipos. Consiste en un software que posibilita la comunicación de un sistema informático con otros equipos en el ámbito de una red.

Familia de Servidores Windows 2003

La familia de servidores Windows 2003 está formada por cuatro versiones:

- Standar edition
- Enterprise edition
- Datacenter edition
- Web edition

Cada una de ellas cuenta con caracteristicas específicas y por lo tanto necesita diferentes requisitos del sistema.

Windows Server 2003, Standard Edition

Esta diseñada para ofrecer servicios y recursos a otros sistemas de una red. Es el sustituto directo de windows NT 4.0 Server y Windows 2000 Server. El sistema operativo incluye un amplio conjunto de caracteristicas y opciones de configuración. Windows Server 2003, standard Edition es compatible con memorias RAM de hasta 4 gigabytes (GB) y dos procesadores.

Windows Server 2003, Enterprise Edition

Amplía las características que incluye la versión Standard, incluyendo soporte para los servicios de metadirectorio y servicios para Macintosh, es compatible con memoria RAM intercambiable en caliente, pueden utilizar hasta 32 GB y 64 GB de RAM y ocho procesadores.

Windows Server 2003, Datacenter Edition

Es el servidor mas robusto, permite el uso de configuraciones de memoria de gran capacidad de hasta 64GB y 128GB de RAM en Itanium. El requisito minimo es de ocho procesadores y puede soportar hasta 32 procesadores en total.

Windows Server 2003, Web Edition

Esta diseñada para proporcionar servicios web para la implantacion de sitios web y aplicaciones basadas en web. Es compatible con memorias RAM de hasta 2 GB y dos procesadores.

Servicios que ofrece windows server 2003

Cualquier servidor puede configurarse para una o varias funciones de servidor. Algunas de esas funciones son:

- **Servidor de aplicaciones:** Un servidor que proporciona servicios web, aplicaciones web y aplicaciones distribuidas.
- **Servidor DHCP:** Un servidor que ejecuta el protocolo DHCP y puede asignar automáticamente direcciones IP a los clientes de la red.
- **Servidor DNS:** Un servidor que ejecuta DNS y resulve los nombres de equipo a direcciones IP y viceversa.
- **Controlador de dominio:** Un servidor que proporciona servicios de directorio para el dominio e incluye un almacén de directorios.
- **Servidor de archivos:** Un servidor que sirve y gestiona el acceso a los archivos.
- **Servidor de correo:** Un servidor que proporciona servicios de correo básicos, para que los clientes de correo puedan enviar y recibir correo en el dominio.
- **Servidor de impresion:** Un servidor que proporciona y administra el acceso a impresoras de red, las colas de impresión y controladores de impresora, permite configurar rápidamnete las impresoras y sus controladores.
- **Servidor de multimedia de transmisión por secuencias:** Un servidor que proporciona contenido multimedia a otros sistemas de la red o de Internet. Esta opcion instala los servicios de Windows Media.

SERVICIOS DE DIRECTORIO

Controlador de dominio

Es un servidor que pertenece a un dominio y contiene una copia de las cuentas de usuario y de otros datos del Directorio Activo. Es obligatorio que haya al menos un controlador de dominio.

Directorio Activo

Es la implementación para Windows de los Servicios de Directorio. Su objetivo fundamental es ampliar las funciones del sistema de dominios para facilitar la gestión y administración de las redes.

Cuenta con las siguientes características:
Incorpora un directorio que almacena datos de los objetos.
Define un catalogo global que contiene información de cada objeto.
Servicio de replicación que distribuye los datos del directorio por toda la red.

Configuracion Básica del Servidor

Modo de Licencia

Los productos de la familia de Windows Server 2003 admiten dos modos de licencia:

- Por servidor
- Por usuario o por dispositivo

Por servidor: Se asigan un número de licencias al servidor que permitirán realizar

conexiones con un determinado recurso del servidor. Cuando un usuario se conecte con un recurso del servidor en dicho servidor, la conexión consumiá una licencia que, cuando dicho usuario se desconecte, quedará libre para su utilización por otro usuario.

Por usuario o por dispositivo: Se requiere una licencia de acceso de cliente (CAL) por cada dispositivo o usuario que se conecte al recurso del servidor seleccionado.Una vez que el dispositivo, o el usuario, disponga de una licencia, puede tener acceso a cualquier servidor en el que se ejecute dicho recurso.

Si no se está seguro del modo de licencia que se necesita, se debe seleccionar Por Servidor.

Sistemas de Archivos

Un sistema de archivos son los métodos y estructuras de datos que un sistema operativo utiliza para seguir la pista de los archivos en una unidad de almacenamiento; es decir, es la manera en la que se organizan los archivos en el disco. Los sistemas de archivos que soporta windows son:

- FAT: Se puede acceder desde MS-DOS y todas las versiones de Windows, no soporta dominios.
- FAT32: Se puede acceder desde Windows 98, 2000, XP, Server 2003. No soporta dominios.
- NTFS: Permite el uso de dominios y directorio activo

Dominios y Grupos de Trabajo

Los dominios y los grupos de trabajo representan diferentes formas de organizar equipos en las redes. La diferencia principal entre ellos es la forma de administrar los equipos y otros recursos de las redes.

Generalmente, los equipos de redes domésticas forman parte de un grupo de trabajo y los equipos de redes de áreas de trabajo forman parte de un dominio.

Dominio:

Es un conjunto de cuentas de usuario y recursos de red bajo un nombre que tiene establecidas fronteras de seguridad.

En un dominio:

·Uno o más equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y los permisos de todos los equipos del dominio.

·Si dispone de una cuenta de usuario en el dominio, puede iniciar sesión en cualquier

equipo del dominio.

·Puede haber cientos o miles de equipos.

Grupo de trabajo:

Es una agrupación básica que unicamente, se establece para ayudar a determinados usuarios a utilizar objetos compartidos.

En un grupo de trabajo:

·Todos los equipos se encuentran en el mismo nivel, ninguno tiene el control sobre otro.

·Cada equipo dispone de un conjunto de cuentas de usuario. para utilizar un equipo del grupo de trabajo, debe disponer de una cuenta en él.

·Normalmente, sólo incluye entre diez y veinte equipos.

·Todos los equipos deben encontrarse en la misma red local o subred.

Controlador de Dominio y Servidor Miembro

Los servidores dentro de un dominio pueden ser:

- **Controlador de Dominio:** pertenece al dominio y contiene una copia de las cuentas de usuario y de otros datos del Directorio Activo. Es obligatorio que haya al menos un controlador de dominio.
- **Servidor miembro:** pertenece al dominio y no contiene una copia de las cuentas de usuario y de otros datos del Directorio Activo. Se utilizan para almacenar archivos y otros recursos.

UNIDAD V

EVALUACION DE LAS NECESIDADES DE LA RED

- Aplicaciones
- Usuarios
- Servicios de red
- Seguridad y protección
- Planeación de la capacidad y crecimiento
- Satisfacción de las necesidades de la red

Cuando se debe diseñar una red, antes de preocuparse de la topología de red que se va a utilizar, qué plataforma de NOS se va a usar, como estructurar los hubs, puentes y demás, qué grado de cableado instalar, es necesario conocer los objetivos que debe alcanzar la red.

Se debe hacer una evaluación de las necesidades de la red, ya que de hacerlo de manera adecuada seguramente traerá como resultado una red que funcione correctamente.

APLICACIONES

Para comenzar el diseño de una red se debe enumerar y comprender las aplicaciones que se deberá correr en la red. La mayoría de las redes tienen tanto aplicaciones comunes como específicas a un departamento o usuario.

Para las aplicaciones comunes se debe considerar los siguientes aspectos:

- Conocer si todos los usuarios requieren todas las aplicaciones instaladas.
- Con que frecuencia planea utilizarlas.

- Cuantos archivos se piensa generar, almacenar y como se compartirán.
- Dentro de estas aplicaciones se encuentran:
- Procesador de palabra
- Hoja de calculo
- Correo electronico
- Software explorador de virus

Para las aplicaciones específicas se debe considerar los siguientes aspectos:

- ¿Qué capacidad de almacenamiento consumirán ?
- ¿Desde dónde se correrá la aplicación?
- ¿Cuanta memoria y ancho de banda necesitará la aplicación?
- Dentro de estas aplicaciones se encuentran:
- Contabilidad
- Nomina
- Publicidad
- Soporte a ventas
- Comercio electónico

USUARIOS

Una vez que se conoce que aplicaciones soportará la red, se puede estimar a cúantos usuarios se necesita dar soporte y qué aplicaciones utilizará cada uno. Requerimientos a tomar en cuenta para los usuarios:

Ancho de Banda:

¿Correran software de videoconferencia a través de la LAN?

¿Enviarán gran cantidad de anexos con mucha frecuencia a través del correo electrónico?

Almacenamiento:

¿Algún grupo de usuarios requiere un nivel de capacidad de almacenamiento mayor al promedio?

Servicios de Red:

¿Algún grupo de usuarios requiere un nivel de sensibilidad que necesite un firewall?

SERVICIOS DE RED

Consiste en determinar los servicios que ofrecerá la red.

Tipos de Servicios:

- Servicios de archivo e impresión
- FTP
- Correo electrónico
- Servicios de respaldo y recuperación
- Servicios centralizados de protección de virus

Para ofrecer cada servicio es necesario conocer:

- Requerimientos de almacenamiento
- Requerimientos de ancho de banda
- Frecuencia de uso
- Usuarios que lo utilizarán

SEGURIDAD Y PROTECCION

La seguridad y protección se vinculan con la necesidad de la compañia de mantener la información segura y en un lugar seguro para que no sufra pérdidas.

Ninguna red está totalmente segura y ninguna información está libre de pérdidas. Sin emnargo, las compañias y departamentos tienen diferentes sensibilidades respecto a estos problemas, lo cual indica que se debe invertir más o menos dinero en estás áreas.

En este punto se debe determinar cuál es la importancia de estos aspectos para la compañia para la que se diseña la red.

PLANEACION DE LA CAPACIDAD Y CRECIMIENTO

El área final que se debe considerar es el crecimiento esperado de la red. Se debe considerar el efecto del crecimiento en las diferentes partes de la red (aplicaciones, usuarios y servicios).

Es importante considerar que los diferentes sistemas operativos de red, topologías y computadoras cliente y servidor afectará, la manera en que una aplicación en particular podrá soportar el crecimiento.

SATISFACCION DE LAS NECESIDADES DE LA RED

Una vez terminado el análisis se podrá comenzar a trabajar en la búsqueda de formas para satisfacer todas la necesidades que se hayan detectado. Este proceso no se lleva

a cabo mediante una serie de pasos, en lugar de ello, se debe comenzar delineando las diferentes partes de la red considerando lo siguiente:

- Selección del tipo de red
- Seleccion de la estructura de la red
- Seleción de los servidores

Y luego construir un panorama completo del diseño de la red.

Selección del tipo de red:

Es muy probable que se desee comenzar el diseño con la selección de un tipo de red, basada en los requerimientos generales de ancho de banda.

Selección de la estructura de red:

En esta etapa se debe decidir como arreglar los hubs, switches, ruteadores que la red necesita, así como la manera en que se cableara la red.

Selección de los servidores:

Para seleccionar los servidores se debe determinar que sistema operativo de red usará, que servicios ofrecerán.

UNIDAD VI

IMPLEMENTACION DE UNA RED CLIENTE SERVIDOR

- Instalación y configuración del servidor
- Administración de cuentas
- Administración de archivos
- Administración de servicios de red

Se debera realizar las practicas del MANUAL PRACTICO DE INTRODUCCION A REDES.

Practica No. 1. Instalacion de windows Server 2003

Realizar la instalacion de Windows Server 2003.

Practica No. 2. Creación de un Controlador de Dominio

Configurar el servidor como Controlador de Dominio

Practica No. 3. Configuración de un Servidor de DHCP

Instalar y configurar el servidor como servidor de DHCP

Practica No. 4. Rellenar Active Directory

Creación de unidades organizativas, cuentas de usuario, cuentas de equipo y cuentas de grupo.

Practica No. 5. Compartir Carpetas y Archivos

Creación de carpetas y archivos compartidos.

Practica No. 6. Conectar una Estación de Trabajo a un Dominio

Conectar una estación de trabajo con Windows XP Professional a un Dominio.

Practica No. 7. Administrando el Equipo

Realizar la administración básica de equipos.