



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 2

1. Redes locales.
 - 1.1. Definición y características de una red local.
 - 1.2. Razones para instalar una red de ordenadores.
 - 1.3. Componentes de una red.
2. Tipología. Medios de transmisión. Métodos de acceso.
3. Dispositivos de interconexión: hubs, bridges, switches, routers.
 - 3.1. Hubs.
 - 3.2. Repetidores (repeaters).
 - 3.3. Puentes (bridges).
 - 3.4. Enrutadores (routers).
 - 3.5. Gateways (pasarelas).
 - 3.6. Switches.
 - 3.7. Sistemas operativos de red.





CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 2

Redes locales. Tipología. Medios de transmisión. Métodos de acceso. Dispositivos de interconexión: Hubs, Bridges, Switches, Routers.

1. REDES LOCALES.

Tras la aparición en 1980 del primer «Pc» se produjo un cambio radical en el manejo de la información disponible en las empresas. Hasta ese momento, la información de las empresas informatizadas era gestionada desde un sistema con un ordenador central, información que era controlada estrictamente por los centros de proceso de datos y que debido a su elevado coste no era accesible a la generalidad de usuarios que la demandaban.

Sin embargo, la aparición de los ordenadores personales supuso una oscilación del péndulo hacia el otro extremo y se generalizó la instalación de infinidad de sistemas de información, de tal modo que cada departamento instalaba sus sistemas individuales y la compartición de la información era muy difícil de alcanzar. Además, cuando se necesitaba encontrar una información de interés era muy probable que se encontrara diseminada por distintos sistemas individuales, lo cual generaba un trabajo adicional cuando no reacciones contra unos sistemas que no aportaban soluciones a las demandas planteadas.

Por ello, a mediados de los años ochenta surgió una tendencia intermedia entre las dos anteriores. Los ordenadores personales se conectarían entre sí, permitiendo que la información se pudiera compartir pero a la vez mantendrían la flexibilidad de que carecían los grandes ordenadores.

Además, habría que tener en cuenta una característica fundamental para comparar las redes frente a los sistemas de grandes ordenadores. Aunque tanto en las redes como en los sistemas de grandes ordenadores los equipos conectados acceden a los recursos de un nodo central, en las redes cada ordenador ejecuta sus procesos mientras que en los grandes sistemas los terminales dependen totalmente del sistema central para llevar a cabo el acceso a los archivos, procesamiento y otras actividades.

De ahí que a las redes se les conozca también como sistemas de proceso distribuido, ya que cada equipo puede cargar los programas en su memoria y ejecutarlos con su procesador. Este hecho permite

que los nodos centrales o servidores puedan optimizarse para la función de archivo, gestión de la red, usuarios, seguridad, etc., al no tener que ocuparse de realizar el procesamiento para los puestos tal y como ocurre en los equipos grandes.

1.1. DEFINICIÓN Y CARACTERÍSTICAS DE UNA RED LOCAL.

Podemos definir una red como un sistema de comunicación que permite conectar ordenadores y otros dispositivos, con el fin de permitir a sus usuarios el acceso a una serie de servicios que van más allá de los que pueden ser prestados directamente por cada uno de los equipos cuando funcionan en modo autónomo. Se habla de red de área local cuando no se requieren los servicios de una red pública de transmisión, es decir, cuando nos referimos al ámbito de una misma oficina, edificio o campus.

Las redes de área local se caracterizan por su alta velocidad, fiabilidad, flexibilidad de instalación, expandibilidad y bajo coste.

A) Alta velocidad.

Velocidades de 10 Mbps son estándar, desde hace tiempo, en redes Ethernet (16 Mbps en Token Ring) frente a velocidades de 32 ó 64 Kbps en redes públicas. Y aunque estas últimas están mejorando su rendimiento (2 Mbps o superiores en RDSI) ya existen velocidades de 100 Mbps en redes FDDI (fibra óptica) o Ethernet (Fast Ethernet y 100Base-VG), más de 600 Mbps en redes ATM (Modo de Transmisión Asíncrona) empezando a utilizarse Giga-Ethernet.

B) Fiabilidad.

Las redes locales son altamente fiables debido a su desarrollo enfocado a la detección y corrección de errores. Además existen sistemas, cada vez más avanzados, de tolerancia a fallos, esto es, mantener la integridad de la red ante daños en sus componentes.

C) Flexibilidad de instalación.

La instalación de una red local puede efectuarse en toda una variedad de condiciones. Las localizaciones pueden incluir desde una sola habitación a varios edificios con diferentes estructuras.

D) Expandibilidad.

Esta característica supone la facilidad de crecimiento que presentan las redes locales. Añadir un equipo o multiplicar el número de ellos, muchas veces sólo dependerá del presupuesto disponible. Además, este crecimiento puede efectuarse modularmente: dependiendo de la estructura inicial, para añadir un equipo probablemente bastará con adquirir una tarjeta y un par de metros de cable.

E) Coste.

El bajo coste de las redes de área local puede considerarse como otra de sus características atractivas.

1.2. RAZONES PARA INSTALAR UNA RED DE ORDENADORES.

Como vimos en la definición del párrafo anterior, red local es sinónimo de conexión entre equipos, derivándose de ello una serie de razones para instalar la misma. Entre ellas podemos citar:

- Compartición de programas y archivos.
- Compartición de los recursos de la red.
- Creación de grupos de trabajo.
- Gestión centralizada.
- Seguridad.
- Otras: correo, acceso a otros sistemas.

1.3. COMPONENTES DE UNA RED.

A) Servidor.

El servidor ejecuta el sistema operativo de red y proporciona los servicios de red a las estaciones de trabajo. Entre estos servicios se incluyen el almacenamiento y gestión de archivos, la gestión de usuarios (altas, bajas, derechos), la seguridad, las órdenes del responsable de la red, etc.

Este equipo debe ser el más potente de la red, con uno o más procesadores Pentium o similar, gran velocidad de acceso a disco, la máxima memoria RAM que se le pueda instalar (min. 64 MB), etc.

B) Estaciones de trabajo.

Son aquellos equipos que se conectan a la red convirtiéndose en un nodo de la misma. Pueden ser equipos con o sin disco duro (arranque remoto), con distintos sistemas operativos: DOS, UNIX, OS/2, etc.

C) Placa de interfaz de red (NIC).

Es la interfaz necesaria para que un Pc se pueda conectar a la red. Esta placa es específica del tipo de red que se está utilizando: Ethernet, Token Ring o ArcNet. El cable de la red se conectará a la parte trasera de la placa, si bien existen redes inalámbricas que funcionan por radio o infrarrojos.

D) Sistema de cableado.

Se explicará más adelante.

E) Recursos compartidos y Periféricos.

Son todos aquellos recursos ligados al servidor, como impresoras, plotters, discos ópticos, CD-Rom, etc., o bien al resto de equipos que puedan ser utilizados por cualquier usuario de la red.

2. TIPOLOGÍA. MEDIOS DE TRANSMISIÓN. MÉTODOS DE ACCESO.

Es necesario conocer una serie de conceptos básicos que vamos a estudiar a continuación.

• CABLEADO.

En primer lugar consideremos los posibles medios físicos de interconexión utilizados en redes locales. Fundamentalmente los medios utilizados son cables de distintos materiales, aunque también se pueden utilizar ondas de radio o rayos infrarrojos. En cuanto al cableado, las posibilidades básicamente son tres, a saber: pares trenzados, coaxiales o fibra óptica.

• PARES DE HILOS TRENZADOS.

Consiste en dos hilos conductores de cobre aislados y trenzados entre sí reduciendo de este modo las interferencias eléctricas. Cuando este cableado está cubierto por una malla protectora, se le denomina «apantallado» o STP en terminología anglosajona. En el supuesto de carecer de dicha malla protectora, se le denomina «sin apantallar» o UTP. Es el cableado típicamente utilizado en las instalaciones telefónicas y aunque presenta limitaciones en cuanto a velocidad de transmisión y alcance (10BaseT, 100 metros) debe considerarse muy seriamente su utilización por las siguientes razones:

- En la mayoría de los casos es el medio más económico.
- En muchos casos se puede utilizar el cableado existente como cable telefónico.
- Satisface las necesidades potenciales de comunicaciones de los usuarios, es fácil de combinar con otros tipos de cable para formar redes extendidas.

Además, desde hace unos años existen nuevas especificaciones que permiten alcanzar velocidades de 100 Mbps:

- La especificación 100Base-TX permite alcanzar dicha velocidad utilizando dos pares de hilos UTP si la calidad del cable es la adecuada: categoría 5.
- La especificación 100Base-T4 define las reglas para poder alcanzar dicha velocidad, utilizando cuatro pares de hilos UTP con una calidad inferior: categoría 3 o superior.

• CABLE COAXIAL.

Son más caros que los pares de hilos, pero soportan mayores velocidades y están menos afectados por perturbaciones exteriores que éstos.

Un cable coaxial consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa puede estar rodeada por una malla metálica (pantalla) para evitar las interferencias. El conjunto está envuelto por una capa protectora. Dentro de los cables coaxiales hay diversos tipos y precios. Generalmente nos referiremos a coaxial grueso o a coaxial fino teniendo más alcance y mayor precio el primero. Así, en redes Ethernet se habla de «Thick Ethernet» o Ethernet grueso -cable amarillo- y de «Thin Ethernet» o Ethernet fino. El primero, también denominado 10Base5, tiene un alcance de 500 metros y una velocidad de 10 Mbps, mientras que el segundo, 10Base2, para una misma velocidad de 10 Mbps sólo permite distancias de hasta 185 metros. Para mayores longitudes se necesita la utilización de Repetidores.

Existen también otros cableados similares, apantallados o no, como pueden ser los RG59, RG62, Twinaxial, etc.

Este tipo de cableado se encuentra hoy en día en franca regresión.

• CABLE DE FIBRA ÓPTICA.

Este tipo de cable transmite señales de datos mediante luz. El sistema de luz más adecuado a este tipo de medio resulta ser el Láser o «Light Amplification by Stimulated Emission of Radiation». La luz modulada pasa por un conductor de vidrio, rodeado por una capa reflectante.

Las velocidades soportadas por este tipo de cables están por encima de las prestaciones actuales en los tipos anteriores de cables. Las velocidades de transmisión de estas redes se encuentran en el rango de los 100 Mbps, pero en algunas aplicaciones especiales se alcanzan velocidades de hasta 500 Mbps. Otra de las ventajas que posee este material es el de permitir alcances de hasta 100 Km. Además, debido a su nula radiación electromagnética poseen una alta seguridad en el mantenimiento de la confidencialidad de la información. Por último, cabría hablar de otros tipos de conexiones, como radio e infrarrojos, pero se emplean solamente en aplicaciones concretas.

• TOPOLOGÍA.

Es la distribución de las conexiones, teniendo que distinguir entre topología física y topología lógica: topología física: forma física de interconexión entre los dispositivos de la red (modo en que se realiza el cableado), topología lógica: flujo de las señales en la red. Para formar una red, los nodos pueden interconectarse de las siguientes formas: red en estrella, red en árbol, red en bus, red en anillo.

– Red en estrella.

En una configuración en estrella, cada estación de trabajo está conectada a un nodo central. El nodo central proporciona el punto lógico para conectar directamente los recursos compartidos más importantes. Generalmente, las estaciones no tienen que tomar decisiones en cuanto a cómo y cuándo transmitir los mensajes, puesto que todas las comunicaciones han de pasar a través del nodo central antes de llegar a sus destinos. El tamaño y capacidad de la red están directamente relacionados con la potencia de la estación central.

1. Ventajas:

- a) Posee una buena flexibilidad en cuanto al incremento y disminución del número de estaciones que se conectan a la red.
- b) Permite una fácil localización de averías.
- c) Se pueden conectar terminales no inteligentes.
- d) Las estaciones de trabajo pueden tener velocidades de transmisión diferentes.
- e) Permite utilizar distintos medios de transmisión.

2. Inconvenientes.

- a) Es susceptible de averías en el nodo central.
- b) Elevado precio debido a la complejidad de la tecnología que se necesita en el nodo central y debido al gran consumo de líneas de conexión.
- c) No permite grandes flujos de tráfico por la posible saturación del controlador.

– Red en bus.

En una configuración en bus, todas las estaciones están conectadas a un único canal de comunicaciones. Para que una estación pueda recibir un mensaje, ésta ha de conocer su propia dirección. Por tanto, los dispositivos conectados a un bus han de disponer de un alto nivel de inteligencia o, de no ser así, la ha de proporcionar la unidad de interfaz.

Puesto que las estaciones más cercanas a la estación emisora reciben una señal más fuerte que las estaciones que se encuentran en el extremo más alejado del bus, la longitud de los segmentos de cable es limitada, pudiendo utilizarse amplificadores de señal para mantener la intensidad de ésta.

1. Ventajas:

- a) La instalación resulta muy sencilla.
- b) Es sencillo conectar nuevos dispositivos.
- c) Se adapta con facilidad a la distribución física de las estaciones.
- d) El coste resulta reducido.

2. Inconvenientes:

- a) Las interfaces para el acceso a la red son muy complejas.
- b) Poca seguridad del sistema, ya que una avería en el soporte físico inhabilita el funcionamiento completo de la red.
- c) A veces se producen bloqueos.

Dentro de la topología en bus distinguiremos entre bidireccional y unidireccional, según que la transmisión se realice en los dos sentidos o en uno solo.

– Red en anillo.

Todas las estaciones están conectadas formando un anillo, de manera que las informaciones atraviesan todas ellas, aunque solamente la estación a la que va dirigida la información puede recuperarla. Para poder recibir mensajes, cada estación ha de ser capaz de reconocer su propia dirección.

1. Ventajas:

- a) La tasa de errores de la transmisión es muy pequeña, ya que la información se regenera en cada nodo de estación.
- b) Se pueden enviar fácilmente mensajes a todas las estaciones.
- c) Diseñada para grandes redes.

2. Inconvenientes:

- a) Una avería en el medio de transmisión o en una estación bloquea la red, aunque para paliar este problema de seguridad se han diseñado redes de doble anillo.
- b) Si el número de estaciones es elevado, el retardo que se produce en la red puede ser grande, ya que cada estación contribuye con un cierto tipo de demora.

• MODULACIÓN.

Es el método de transmisión o proceso necesario para que la señal digital pueda pasar a través del medio físico de transmisión. Existen dos tipos fundamentales de modulación que son:

a) Banda base.

La señal digital sin sufrir ningún proceso de modulación se aplica directamente al medio físico de transmisión, que no transmite simultáneamente más que esa señal. Este modo es el más económico ya que utiliza dispositivos electrónicos sencillos para la transmisión y recepción de datos, pero tiene el inconveniente de que la velocidad que soporta es limitada.

b) Banda ancha.

En este caso la señal digital es modulada sobre una portadora que se aplica al medio de transmisión. Con este sistema se pueden transmitir simultáneamente varias portadoras multiplexadas por división de frecuencias, lo que supone que se dispone de varios canales de transmisión sobre los que se puede transferir datos, voz y vídeo simultáneamente. Este modo es más caro que la banda base, pero puede ser económicamente más rentable si se aprovecha su capacidad de comunicación simultánea de la voz e imágenes además de los datos. Se exige que las estaciones se conecten a través de modems. Los sistemas ópticos trabajan modulando en amplitud el rayo de luz que pasa a través de la fibra óptica. En general utilizan señalización en banda base, en la que la forma de variación de la luz es similar a la tensión en los sistemas eléctricos con cables conductores.

• CODIFICACIÓN.

Este concepto se refiere al modo en que se transmiten los bits de información a través del cable. El método más sencillo es el NRZ (Non Return to Zero) en el que cada bit se representa por un estado determinado de la señal. Este sistema tiene problemas para la sincronización en recepción, por lo que en muchos casos se emplean otros sistemas que facilitan la sincronización del receptor como son el NRZI (Non Return to Zero Inverted) y el Código Manchester.

• MÉTODOS DE ACCESO.

Éste es un concepto particular de las redes locales y se refiere al sistema que emplean para arbitrar la utilización de los medios de comunicaciones.

Uno de los métodos posibles es la contención, en donde cada una de las estaciones puede transmitir información en cualquier momento siempre que se encuentre libre el medio de comunicación. En este caso se tiene el problema de que pueden ocurrir colisiones, por lo que será necesario disponer de una serie de mecanismos que permitan salvar esta situación.

Otra forma de arbitraje es la utilización de un testigo, que consiste en un mensaje especial que se va pasando de estación a estación. Cada estación puede transmitir su mensaje solamente cuando está en posesión del testigo, cosa que ocurre cuando recibe lo que se denomina el testigo libre. Los testigos pueden ser de diversos tipos, dependiendo de la red local. Un testigo libre puede ser un mensaje de algunos caracteres que se intercambian las estaciones.

Cuando una estación que quiere transmitir recibe el testigo libre, genera un testigo ocupado. En éste se incluyen las direcciones de la estación origen y destino y precede a los datos. En algunos casos se utiliza una secuencia de bits determinada, llamada preámbulo, que permite la inicialización de los circuitos de la estación receptora. Para evitar situaciones de bloqueo debido al tipo de operación del paso de testigo, las redes que utilizan este método de acceso suelen tener una estación que hace de controlador de situaciones de error.

Las dos técnicas más utilizadas actualmente son el acceso múltiple por detección de portadora CSMA (Carrier Sense Multiple Access) y el de PASO DE TESTIGO (Token Passing), denominaciones que se refieren al método de acceso y no al formato de datos. El modo de trabajo de ambos se describe a continuación:

A) CSMA.

En el protocolo CSMA los nodos están continuamente a la escucha para detectar cualquier dato que se les haya dirigido. Para poder transmitir es necesario en primer lugar asegurarse de que no hay ninguna señal presente en el medio físico y cuando no detecta portadora puede pasar a transmitir.

Dentro de CSMA se pueden utilizar dos sistemas distintos, que son detectar la colisión (CSMA/CD: collision detection) y evitar la colisión (CSMA/CA: collision avoidance).

a) Detectar la colisión.

Es el más utilizado. Debido a que es posible que dos equipos se pongan a transmitir simultáneamente cuando no hay portadora se debe controlar la posible colisión de señales. Cuando un nodo detecta una colisión al intentar transmitir, espera un cierto tiempo predefinido por un algoritmo de contención y vuelve a intentar la transmisión de nuevo.

b) Evitar la colisión.

Suele basarse en sistemas de división en el tiempo de acuerdo con los cuales cada nodo espera un período de tiempo predefinido antes de intentar la transmisión, teniendo cada uno de los nodos un período diferente.

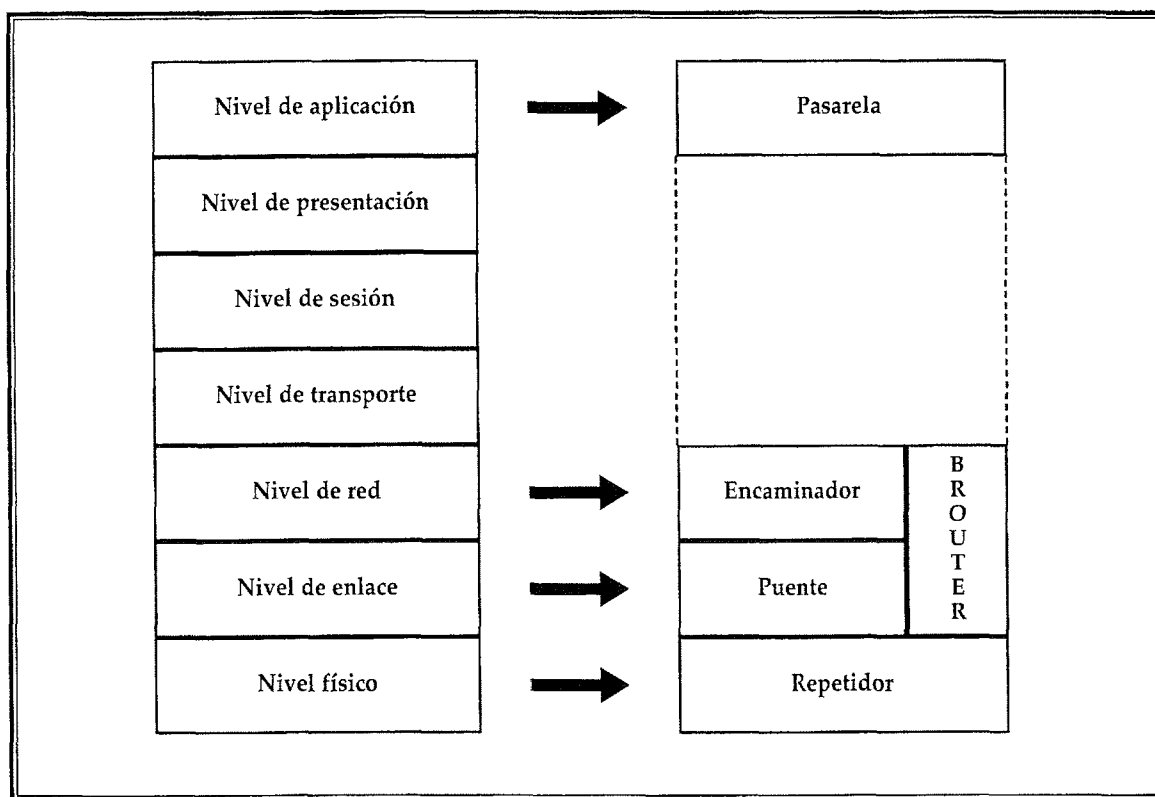
B) Paso de testigo.

Este sistema evita que traten de comunicarse más de un nodo simultáneamente pasando un paquete especial llamado testigo, a través de la red, siendo este testigo el que da el permiso de transmitir. Cuando un equipo quiere comunicarse, debe coger previamente el testigo y cuando termina libera el testigo de modo que se puede establecer una nueva comunicación.

Captura de testigo. Este sistema, utilizado en las redes FDDI, es parecido al método anterior con la salvedad de que para transmitir no hay que esperar a que quede libre el testigo, simplemente se añade la información al testigo que circula.

3. DISPOSITIVOS DE INTERCONEXIÓN: HUBS, BRIDGES, SWITCHES, ROUTERS.

En la siguiente figura se representa la relación de los dispositivos de interconexión con los niveles del modelo de referencia OSI.

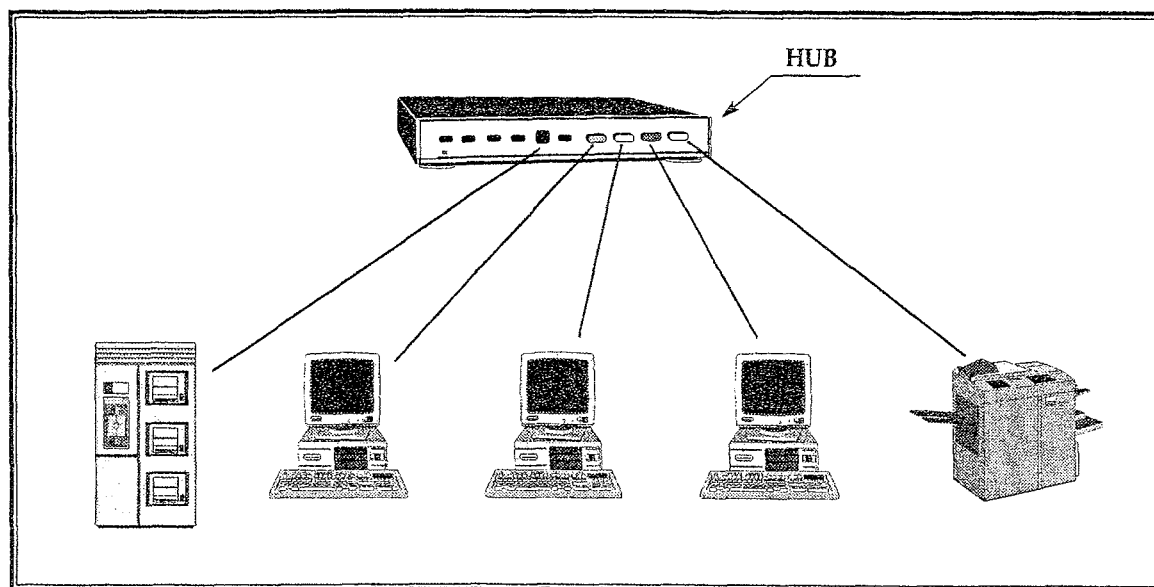


Ateniéndonos a los niveles que soporten los dispositivos de interconexión para redes locales dentro de la arquitectura OSI y de menor a mayor, podemos considerar las siguientes clases:

3.1. HUBS.

Son puntos de conexión para los dispositivos que se encuentran en una red. Los hubs se utilizan normalmente para conectar segmentos de una red local. Un hub contiene múltiples puertos, cuando llega un paquete a un puerto se copia el mismo paquete a los otros puertos y así todos los segmentos

de la red pueden ver todos los paquetes. Hay dos tipos de hubs: hubs pasivos que efectúan la función indicada anteriormente y hubs activos que permiten al administrador de red monitorizar el tráfico así como configurar el tráfico de cada puerto.



Los nuevos hubs de «tercera generación» ofrecen proceso basado en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes: Ethernet, Token Ring, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

A un hub Ethernet se le denomina «repetidor multipuerta». El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del hub. En el otro extremo de cada cable está un nodo de la red, por ejemplo, un ordenador personal. Un hub Ethernet se convierte en un hub inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control.

Los concentradores inteligentes (smart hubs) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. La capacidad de gestión remota de los hubs inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la RAL, con lo que otros usuarios no se ven afectados.

El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

3.2. REPETIDORES (REPEATERS).

Funcionan en el nivel físico, es decir, manejando los bits. Permiten adaptar diferentes medios físicos para su utilización en una red local o aumentar la distancia que permite el cable utilizado. Un dispositivo de este tipo sería un convertidor de cable coaxial a fibra óptica que puede tener una gran utilidad para aislamiento galvánico de tramos de red.

3.3. PUENTES (BRIDGES).

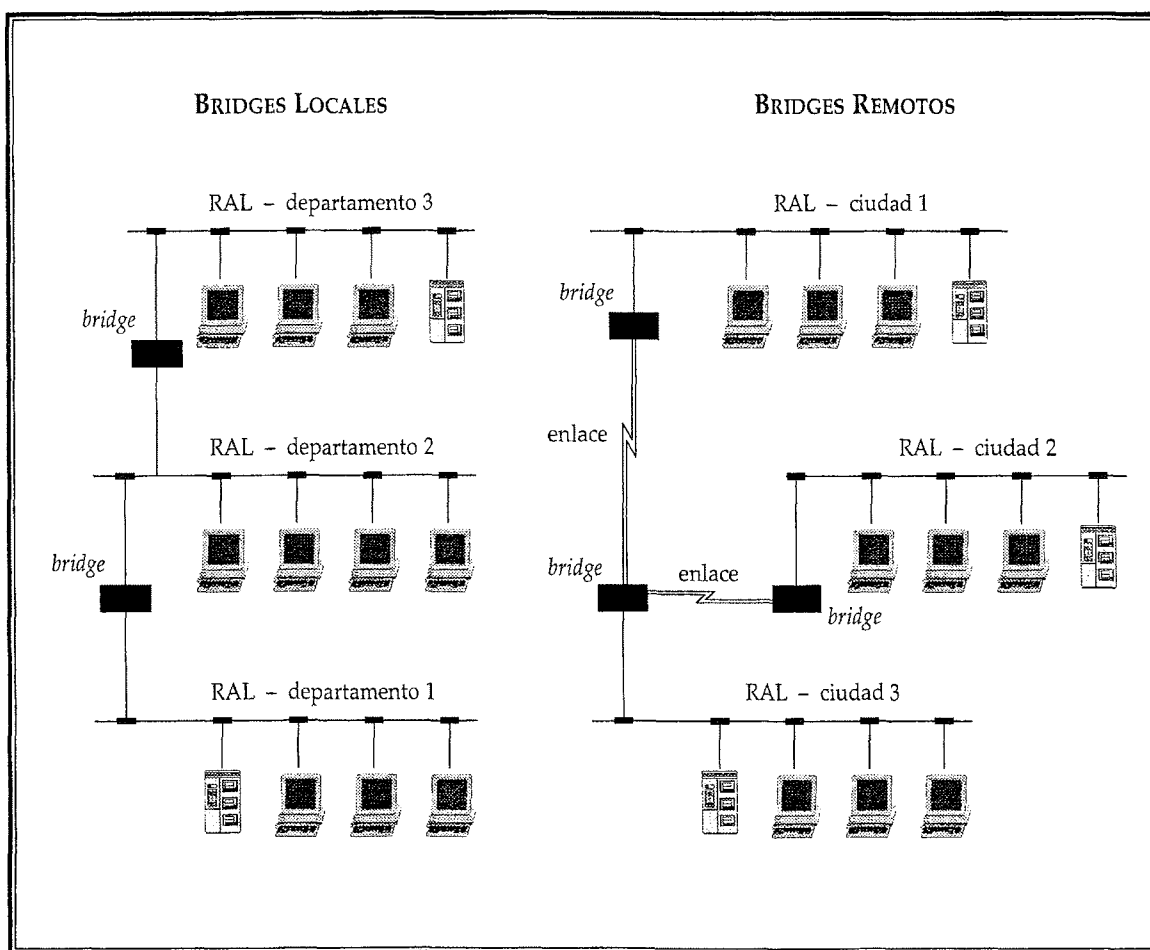
Incorporan hasta el nivel de enlace (2). Son equipos que conectan dos redes que utilizan protocolos similares o idénticos. También permiten la interconexión de redes locales que utilizan distinto medio físico o diferente método de acceso. No realizan conversión de protocolo ni de código, pero pueden cambiar la velocidad y soportar control de flujo, por lo que ambas redes deben utilizar los mismos protocolos en los niveles superiores.

Un bridge 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 distinguen dos tipos de bridges:

- Locales: sirven para enlazar directamente dos redes físicamente cercanas.
- Remotos o de área extensa: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.



Se puede realizar otra división de los bridges en función de la técnica de filtrado y envío (*bridging*) que utilicen:

- Spanning Tree Protocol Bridge o Transparent Protocol Bridge (Protocolo de Árbol en Expansión o Transparente, STP).

Estos bridges deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

- Source Routing Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor, SRP).

El emisor ha de indicar al bridge cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos Token Ring.

- Source Routing Transparent Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor Transparente, SRTP).

Este tipo de bridges puede funcionar en cualquiera de las técnicas anteriores.

Ventajas de la utilización de bridges:

- Fiabilidad. Utilizando bridges se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- Eficiencia. Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- Seguridad. Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- Dispersión. Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los bridges permiten romper esa barrera de distancias.

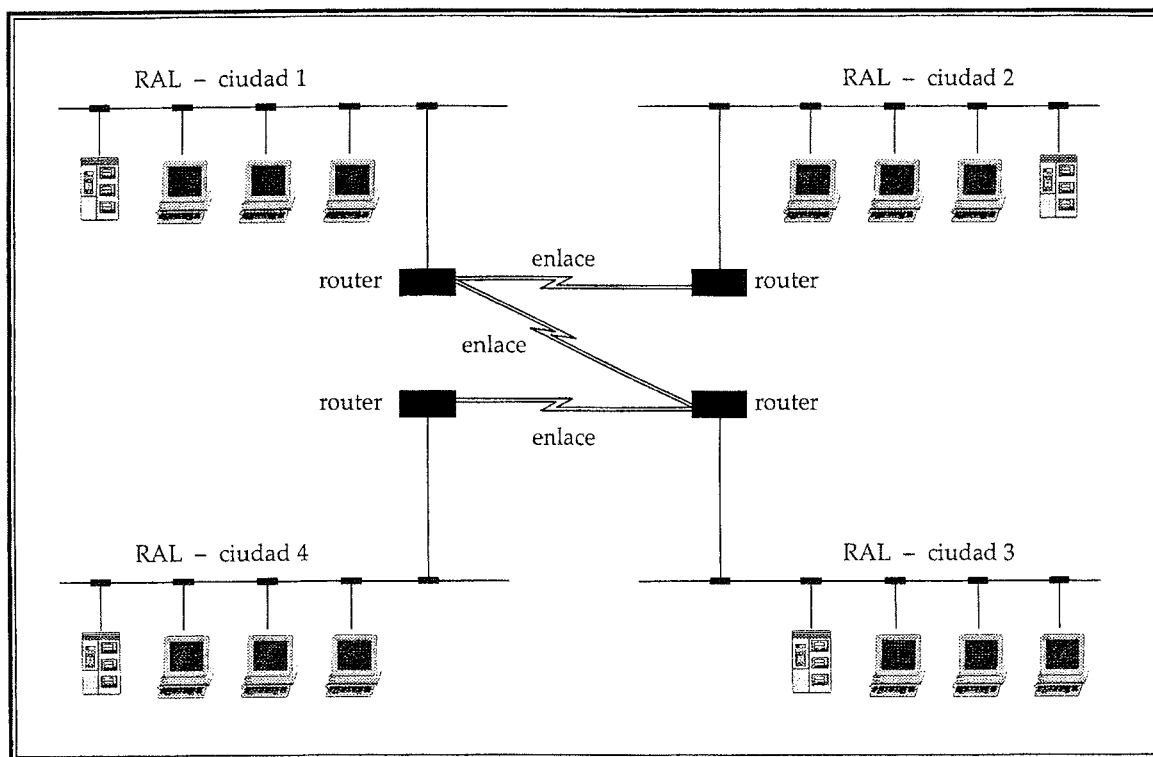
Desventajas de los bridges:

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios bridges.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

Las aplicaciones de los bridges está en soluciones de interconexión de RALs similares dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento y transparencia a los protocolos de niveles superiores. También son útiles en conexiones que requieran funciones de filtrado. Cuando se quiera interconectar pequeñas redes.

3.4. ENRUTADORES (ROUTERS).

Soportan hasta el nivel de red y permiten la conexión de varias redes en un punto común. En redes de conmutación de paquetes X.25, estos dispositivos son los nodos de red. Convierten los paquetes de información de la red de área local en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el encaminador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás routers para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre routers se realiza mediante protocolos de gestión propietarios.



Los encaminadores se pueden clasificar dependiendo de varios criterios:

- En función del área:
 - Locales: sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al router.
 - De área extensa: enlazan redes distantes.
- En función de la forma de actualizar las tablas de encaminamiento (routing):
 - Estáticos: la actualización de las tablas es manual.
 - Dinámicos: la actualización de las tablas las realiza el propio router automáticamente.

- En función de los protocolos que soportan:

- IPX.
- TCP/IP.
- DECnet.
- AppleTalk.
- XNS.
- OSI.
- X.25.
- Etcétera.

- En función del protocolo de encaminamiento que utilicen:

- Routing Information Protocol (RIP).

Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de encaminamiento dinámicas y se intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

- Exterior Gateway Protocol (EGP).

Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes routers para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

- Open Shortest Path First Routing (OSPF).

Está diseñado para minimizar el tráfico de encaminamiento, permitiendo una total autenticación de los mensajes que se envían. Cada encaminador tiene una copia de la topología de la red y todas las copias son idénticas. Cada encaminador distribuye la información a su encaminador adyacente. Cada equipo construye un árbol de encaminamiento independientemente.

- IS-IS.

Encaminamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de encaminamiento en un dominio y entre diferentes dominios. Dentro de un mismo dominio el encaminamiento se realiza aplicando la técnica de menor coste. Entre diferentes dominios se consideran otros aspectos como puede ser la seguridad.

Otras variantes de los routers son:

- Router Multiprotocolo.

Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los routers de segunda generación. No es necesario, por tanto, tener un router por cada protocolo de alto nivel existente en el conjunto de redes interconectadas. Esto supone una reducción de gastos de equipamiento cuando son varios los protocolos en la red global.

- Brouter (bridging router).

Son routers multiprotocolo con facilidad de bridge. Funcionan como router para protocolos encaminables y, para aquellos que no lo son se comportan como bridge, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones.

Operan tanto en el nivel de enlace como en el nivel de red del modelo de referencia OSI. Por ejemplo, un brouter puede soportar protocolos de encaminamiento además de source routing y spanning tree bridging. El brouter funciona como un router multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como bridge.

Las características y costes de los brouters hacen de éstos la solución más apropiada para el problema de interconexión de redes complejas. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo, source routing y spanning tree e incluso de protocolos no encaminables. Son aconsejables en situaciones mixtas bridge/router. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo.

- Trouter.

Es una combinación entre un router y servidor de terminales. Permite a pequeños grupos de trabajo la posibilidad de conectarse a RALs, WANs, modems, impresoras, y otros ordenadores sin tener que comprar un servidor de terminales y un router. El problema que presenta este dispositivo es que al integrar las funcionalidades de router y de servidor de terminales puede ocasionar una degradación en el tiempo de respuesta.

Ventajas de los routers:

- Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
- Flexibilidad. Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.
- Soporte de protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- Relación precio/eficiencia. El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.

- Control de flujo y encaminamiento. Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc.), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas de los routers:

- Lentitud de proceso de paquetes respecto a los bridges.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los bridges.

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de RALs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

3.5. GATEWAYS (PASARELAS).

Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (Nivel de Transporte, Sesión, Presentación y Aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes.

Los gateways incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un bridge o un router, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos.

Los gateways tienen mayores capacidades que los routers y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

A continuación se describen algunos tipos de gateways:

- Gateway asíncrono.

Sistema que permite a los usuarios de ordenadores personales acceder a grandes ordenadores (mainframes) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas conmutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.

- Gateway SNA.

Permite la conexión a grandes ordenadores con arquitectura de comunicaciones SNA (System Network Architecture, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.

- Gateway TCP/IP.

Estos gateways proporcionan servicios de comunicaciones con el exterior vía RAL o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.

- Gateway PAD X.25.

Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.

- Gateway FAX.

Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

Ventajas:

- Simplifican la gestión de red.
- Permiten la conversión de protocolos.

Desventajas:

- Su gran capacidad se traduce en un alto precio de los equipos.
- La función de conversión de protocolos impone una sustancial sobrecarga en el gateway, la cual se traduce en un relativo bajo rendimiento. Debido a esto, un gateway puede ser un cuello de botella potencial si la red no está optimizada para mitigar esta posibilidad.

Su aplicación está en redes corporativas compuestas por un gran número de RALs de diferentes tipos.

3.6. SWITCHES.

Los conmutadores tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos. Esto es posible debido a que los equipos configuran unas tablas de encaminamiento con las direcciones MAC (nivel 2 de OSI) asociadas a cada una de sus puertas.

Esta tecnología hace posible que cada una de las puertas disponga de la totalidad del ancho de banda para su utilización. Estos equipos habitualmente trabajan con anchos de banda de 10 y 100 Mbps, pudiendo coexistir puertas con diferentes anchos de banda en el mismo equipo.

Las puertas de un conmutador pueden dar servicio tanto a puestos de trabajo personales como a segmentos de red (hubs), siendo por este motivo ampliamente utilizados como elementos de segmentación de redes y de encaminamiento de tráfico. De esta forma se consigue que el tráfico interno en los distintos segmentos de red conectados al conmutador afecte al resto de la red aumentando de esta manera la eficiencia de uso del ancho de banda.

Hay tres tipos de conmutadores o técnicas de conmutación:

- Almacenar–Transmitir. Almacenan las tramas recibidas y una vez chequeadas se envían a su destinatario. La ventaja de este sistema es que previene del malgasto de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa ligeramente el tiempo de respuesta del switch.
- Cortar–Continuar. En este caso el envío de las tramas es inmediato una vez recibida la dirección de destino. Las ventajas y desventajas son cruzadas respecto a Almacenar–Transmitir. Este tipo de conmutadores es indicado para redes con poca latencia de errores.
- Híbridos. Este conmutador normalmente opera como Cortar–Continuar, pero constantemente monitoriza la frecuencia a la que tramas inválidas o dañadas son enviadas. Si este valor supera un umbral prefijado, el conmutador se comporta como un Almacenar–Transmitir. Si desciende, este nivel se pasa al modo inicial.

En caso de diferencia de velocidades entre las subredes interconectadas el conmutador necesariamente ha de operar como Almacenar–Transmitir.

Esta tecnología permite una serie de facilidades tales como:

- Filtrado inteligente. Posibilidad de hacer filtrado de tráfico no sólo basándose en direcciones MAC, sino considerando parámetros adicionales, tales como el tipo de protocolo o la congestión de tráfico dentro del switch o en otros switches de la red.
- Soporte de redes virtuales. Posibilidad de crear grupos cerrados de usuarios, servidos por el mismo switch o por diferentes switches de la red, que constituyan dominios diferentes a efectos de difusión. De esta forma también se simplifican los procesos de movimientos y cambios, permitiendo a los usuarios ser ubicados o reubicados en red mediante software.
- Integración de routing. Inclusión de módulos que realizan función de los routers (encaminamiento), de tal forma que se puede realizar la conexión entre varias redes diferentes mediante propios switches.

3.7. SISTEMAS OPERATIVOS DE RED.

Un sistema operativo de red es un conjunto de programas que permite a los usuarios compartir archivos y recursos. Se puede hablar de dos tipos básicos de sistemas operativos de red en función de la existencia o no de un equipo, o varios, con características y funciones claramente diferenciadas del resto. Así, podemos hablar de «punto a punto» o «con servidores dedicados».

La diferencia fundamental es que en el primer caso el SO de red (NOS en inglés) se ejecuta en los ordenadores de los usuarios individuales, mientras que en el segundo caso se ejecuta en un ordenador dedicado, que se dedica exclusivamente para tareas de red como facilitar la comparación de archivos, recursos, gestión de usuarios, seguridad, etc.

Ejemplos del primer tipo de NOS serían las redes montadas entre equipos en los que se ejecutan Windows 2000 Home o Profesional o Windows XP. En estas redes los usuarios pueden compartir los recursos de sus ordenadores a la vez que acceden a los recursos de otros equipos de la red: discos duros, impresoras asociadas a ellos, etc.

En el segundo tipo de NOS estaría claramente situado Novell NetWare en todas sus versiones, siendo un sistema donde la información está centralizada en el servidor o servidores, existiendo una política global de accesos, seguridad, disponibilidad de recursos, etc., para todos los usuarios de la red. También encuadraríamos en este apartado el SO de Microsoft Windows NT, así como WINDOWS 2000 SERVER y LINUX ya que aunque permite utilizar el servidor como un puesto más de la red su verdadera función es la reseñada más arriba. Podríamos por tanto hablar de un entorno cliente-servidor, entendiendo como cliente un puesto de la red -o nodo- que accede a servicios de la misma, en el que la interacción del usuario ocurre vía peticiones de servicios o recursos por parte del cliente, a las cuales el servidor responde.

El papel de servidor puede ser llevado a cabo por diferentes sistemas, incluyendo ordenadores personales corriendo software especializado para servicios de red. Este tipo de software es llamado Sistema Operativo de Red (NOS: Network Operating System).

Por otra parte, el hecho de haber realizado la diferenciación anterior no impide el que nos encontremos con entornos mixtos, es decir, que ambos sistemas operativos puedan coexistir en una misma red. En este supuesto, dos usuarios pueden compartir los discos de sus equipos individuales a la vez que comparten el uso de una base de datos en el servidor dedicado. Es importante recalcar la posibilidad apuntada en el párrafo anterior de la capacidad, por parte de los servidores dedicados, de ejecutar aplicaciones multiusuario en las que numerosos usuarios acceden a recursos o información en un punto común. Una ventaja añadida a la posibilidad de compartir dicha información es la de facilitar a los administradores la implantación de una política de seguridad, auditoría, etc. En una palabra: facilita la gestión de la red. En los sistemas punto a punto, sin embargo, la gestión es mucho más difícil ya que los datos y los recursos se encuentran dispersos por toda la red.

Por último, habría que destacar una serie de servicios clave que cualquier sistema operativo debe ofrecer para soportar a los usuarios de una red:

• SERVICIOS QUE PROVEEN.

A) Ficheros.

El servicio de ficheros permite a los usuarios el acceso a directorios y archivos concretos, de un determinado servidor, en función de los derechos que tengan asignados sobre los mismos. La manera de facilitar ese acceso, así como las posibles limitaciones a efectuar alteraciones a aquéllos, restricciones del espacio disponible, posibilidad de recuperar ficheros/directorios borrados, optimización de la búsqueda, escritura o recuperación de los mismos son características consustanciales con cada sistema operativo de red.

Así, por ejemplo, tanto Novell NetWare, desde la versión 4.0, como Windows NT (formateado como NTFS) implementan un sistema de compresión de ficheros que permite ahorros de disco superiores en un 50 por 100. Mediante este sistema los archivos no utilizados, desde un período de tiempo configurable, se comprimen hasta el momento de ser solicitada su apertura nuevamente. Otra característica, específica de Novell, es la limitación de espacio en disco disponible por un usuario.

B) Impresoras.

Mediante este servicio se facilita la impresión compartida de manera que los usuarios de la red puedan acceder a las impresoras conectadas a la misma sin importar su tipo o forma de conexión. Así, por ejemplo, Novell NetWare soporta hasta 256 impresoras conectadas en sus versiones 4.x.

Estas impresoras pueden estar soportadas por uno o varios servidores de impresión que, a su vez, pueden instalarse en el servidor de ficheros, en una estación remota o estar soportadas, valga la redundancia, en una serie de dispositivos autónomos que realizan toda la gestión de los trabajos asignados a las impresoras dependientes de los mismos. Sería el caso de las tarjetas JetDirect de Hewlett Packard que permiten una gestión de la impresión sin necesidad de hacerlo desde el Servidor Novell o Windows NT.

El mecanismo de trabajo se basa en el sistema de colas de impresión, de tal modo que un usuario manda un trabajo a una cola y es el servidor de impresión, en cualquiera de las acepciones vistas en el párrafo anterior, el que se encarga de dirigirlo a la impresora adecuada regulando el «tráfico» e indicando mediante los mensajes oportunos las posibles incidencias aparecidas en el proceso de impresión.

C) Seguridad.

Este tema se puede abordar desde dos puntos de vista: protección de datos, es decir, seguridad de que los datos no sufran alteraciones durante el funcionamiento del sistema, y seguridad en los accesos, esto es, garantizar el acceso a los recursos únicamente a los usuarios que tengan derecho sobre los mismos.

Como ejemplos de mecanismos para proteger la integridad de los datos se encuentran la verificación de lectura tras la escritura, proceso que efectúa la lectura de lo que se acaba de escribir en el disco comparándolo con lo que tiene en memoria de tal modo que si se detecta un error los datos son nuevamente escritos, «Duplicación de FAT» y «Directorios», permitiendo disponer de copias de seguridad de dicha información básica, «Tolerancia a fallos», mediante la posibilidad de contar con discos donde replicar la información (discos espejo o «mirroring») e incluso servidores duplicados (CSFT-III de Novell NetWare) o sistemas de alta disponibilidad (Clusters en Windows NT).

Si tenemos en cuenta la seguridad en los accesos todos los sistemas cuentan con una «cuenta» con su correspondiente clave de acceso o «password». En esa cuenta se definen los perfiles del usuario, es decir, cómo, cuándo y dónde puede acceder, así como qué puede hacer. Un ejemplo sencillo de lo anterior es la autorización dada a un usuario de «solo lectura» sobre un archivo lo cual implica que ese usuario podrá ver el contenido de ese archivo pero no podrá modificarlo. La diferencia entre los distintos SO de red estriba en la manera de establecer esos derechos ya que, por ejemplo, Novell permite restricciones de espacio en disco por usuario mientras que Windows NT no lo hace. Por último habría que mencionar la seguridad de la red a nivel de certificaciones, es decir, cumpliendo las exigencias de la Administración Norteamericana, de manera que tanto Novell como Microsoft cumplen las normas C2 que garantizan a la red como un sistema seguro.

D) Mensajería.

Con este servicio se proporcionará transmisión y almacenamiento de mensajes en la red, teniendo en cuenta que la red puede ser local o tan amplia como queramos incluyendo Internet. Microsoft dispone del «Microsoft message queue server», mientras Novell proporciona, como producto opcional, GroupWise.

Con estos productos se proporcionan, entre otras, las funciones de Buzón Universal, Gestión de mensajes, Filtros, Notificaciones y Alarmas, Integración de correo vocal, imágenes, etc.

E) Enrutado.

El enrutado, «routing» en inglés, permite comunicaciones entre redes, de forma que dichas redes aparecen como una sola para el usuario. Con este servicio se puede acceder, por ejemplo, desde un puesto de una red local NetWare o NT en una ciudad a un equipo Unix en otra ciudad vía X-25. Para cumplir estas funciones Novell incorpora el Router Multiprotocolo, mientras Microsoft lo hace con el Servicio de acceso remoto avanzado (RAS).

F) Gestión.

Servicio que permite la administración de la red mediante una serie de utilidades incorporadas en el Sistema. Novel cuenta con el NWAdmin como herramienta básica, mientras Microsoft incluye el conjunto denominado Windows NT Administrative Tools.

G) Publicación Web.

Este servicio permite publicar información en un servidor Web de manera privada (Intranet), o en Internet, como World Wide Web. También se incluyen servicios de transferencia de ficheros FTP con TCP/IP.

Con el servicio de Web se podrá publicar información estática en modo de documentos HTML, o se podrán utilizar entornos de programación L-CGI y R-CGI (CGI = Common Gateway Interface), intérprete NetBasic, soporte de Java, Java Scripts (Netscape), Active-X (Microsoft), etc. Este servicio se proporciona por Novell, con su Web Server, y por Microsoft con su Internet Information Server (IIS).

H) Directorios/Dominios.

Este servicio es clave ya que supone la forma de organizar, acceder y controlar los recursos de la red siendo el aspecto que más distingue a Novell y Microsoft en la forma de entender el sistema operativo de red.

Novell entiende la organización de la red de manera jerárquica, como un árbol, donde todos los elementos de la misma, objetos, son ramas u hojas de ese árbol simplificando enormemente la gestión ya que los derechos se asignan al árbol, con todas las restricciones que sean necesarias a los objetos, de modo que si existen varios servidores en el árbol no hay que manejar los usuarios más que una vez, al contrario que sucede con el sistema de Dominios de Windows NT basado en una estructura plana, que obliga a una gestión menos ágil debido a las múltiples relaciones que deben establecerse entre los servidores.

I) WINDOWS NT.

Windows NT aparece en el mercado como la primera propuesta de la empresa Microsoft de construir un sistema operativo serio capaz de competir con UNIX. La arquitectura de este sistema operativo no tiene nada que ver con el otro sistema operativo de Microsoft para aplicaciones de 32 bits. Uno de los objetivos principales que se propone Microsoft con el diseño de este sistema operativo es que posea un núcleo tan pequeño como fuera posible y que en él estuviera integrado alguno de los módulos que dieran respuesta a algunas llamadas que necesariamente se tuvieran que ejecutar en modo privilegiado y que las demás llamadas fueran atendidas por otras entidades. De esta forma se conseguiría tener un núcleo compacto y estable.

Para realizar este diseño Microsoft se basa en el modelo cliente servidor donde el kernel se encarga de recibir llamadas y pasarlas a procesos servidores que se encargan de ejecutarlas. En Windows NT todos son objetos los cuales poseen unos atributos y unas funciones específicas que se encargan de modificar estos atributos. Los objetos son ficheros, procesos y dispositivos físicos. En Windows las llamadas al sistema reciben el nombre de API. Estas llamadas al sistema en Windows NT son atendidas principalmente por subsistemas. Existen varios subsistemas encargados de ejecutar las llamadas al sistema. Estos son:

El Subsistema Win32 el cual es el más importante de todos ya que no sólo atiende las aplicaciones nativas de Windows NT, sino que para aquellos programas no Win32 reconoce su tipo y los lanza hacia el subsistema. Este subsistema soporta una buena parte del Api Win32 y se encarga de todo lo relacionado con la interfaz gráfica con el usuario (GUI), controlando las entradas del usuario y las salidas de la aplicación. Por otra parte tenemos el subsistema Posix y el OS/2 que se ejecutan interactuando con el Executive y se encargan de proporcionar soporte para aplicaciones Unix y OS/2 respectivamente. Por último tenemos dos subsistemas más que son el de proceso de inicio que se encarga de gestionar los usuarios locales así como los remotos, y el subsistema de seguridad que interacciona con el de proceso de inicio atendiendo las peticiones de acceso al sistema.

Por otra parte tenemos el executive que no se trata del núcleo del sistema sino que dentro de él se encuentra el núcleo del sistema, pero aparte está formado por otros servidores o administradores que se encargan también de recibir las llamadas al sistema. Dentro de estos administradores tenemos el administrador de objetos, que se encarga de crear, destruir y gestionar todos los objetos. Como he dicho antes en Windows NT la gran mayoría de cosas son objetos, los procesos, los subprocesos, ficheros, segmentos de memoria, etc. Por esto existen llamadas que permiten crear y destruir objetos y éstas van a ser atendidas por este servidor. También posee un administrador de procesos que, en colaboración que el administrador de objetos se encarga de crear, destruir y gestionar los procesos y los subprocesos.

Continuando con los administradores contenidos en el Executive también nos encontramos un administrador de memoria virtual que se encarga de gestionar la memoria.

Otro de los administradores importantes es el administrador de entrada salida. Este administrador se encarga de la gestión de la comunicación entre los distintos drivers de dispositivo. Este subsistema contiene dentro de él el administrador del sistema de ficheros. Este administrador se encarga de gestionar el sistema de ficheros de Windows NT.

El núcleo de Windows NT se incluía dentro del executive. En Windows NT el núcleo lleva a cabo las operaciones más fundamentales, determinando cómo el sistema operativo utiliza el procesador o procesadores, asegurando que se utilizan prudentemente. El éxito del sistema operativo completo depende de una correcta y eficiente operación del núcleo.

El núcleo está separado del executive, implementando los mecanismos de sistema operativo y evitando hacer cualquier tipo de políticas. Deja todas las decisiones al executive de Windows NT. Separar los mecanismos de sistema operativo de sus políticas es un principio importante en Windows NT. Los mecanismos se refieren a la forma en la cual se realizan las tareas en un sistema, y están implementados por algoritmos y código. Las políticas determinan qué tareas se deben realizar y cuándo, o incluso se deben realizar ciertas tareas. El principio de separar las políticas de los mecanismos existe en varios niveles en Windows NT.

En el nivel más alto cada subsistema de entorno establece una capa de políticas de sistema operativo que es distinta en cada subsistema. Bajo los subsistemas, el executive de Windows NT establece otra capa más básica de políticas que se ajusta a todos los subsistemas. En la capa más baja del sistema operativo, el núcleo evita las políticas enteramente, él mismo sirve como una capa entre el resto del sistema operativo y el procesador. Forzar a que todas las operaciones relacionadas con el procesador sean canalizadas a través del núcleo resulta en una gran portabilidad y predicibilidad. El executive de Windows NT ejerce sólo un control limitado sobre estas operaciones al llamar a las funciones del núcleo.

J) WINDOWS 2000.

a) Introducción.

Windows 2000 es la última versión de Windows de la empresa Microsoft que tiene como objetivo dar una mayor facilidad de configuración y administración, estabilidad, escalabilidad y rendimiento. Obtiene un mayor rendimiento global con 64 MB o más de memoria RAM. Tiene soporte de procesador y memoria escalable que llega hasta 4 GB de RAM y hasta dos multiprocesadores simétricos.

Windows 2000 mejora el soporte para hardware de la próxima generación, ofreciendo una mayor capacidad de Plug & Play, ya que instala y configura automáticamente los drivers durante el Setup y cada vez que se añada o quite hardware.

b) Directorio activo.

El servicio de directorios es una de las principales novedades del sistema, lo que permitirá cubrir una buena parte de las necesidades de gestión de los administradores. La idea es construir un repositorio centralizado en el cual almacenar toda la información relevante de la empresa en cuanto a su estructura: usuarios, contraseñas, privilegios, direcciones, configuraciones.

Esta información es accedida desde multitud de puntos y muchas veces al día; como la información que necesitamos acceder se encuentra en multitud de lugares genera una dificultad enorme su administración. Básicamente sirve para convertir nombres de dominio en direcciones de máquina. Tiene dos características muy importantes:

- Define un protocolo y una interfaz que nos permiten hacer uso del mismo de una forma independiente del sistema operativo.
- Tiene una estructura jerárquica y distribuida que permite que cada organización administre la información de forma independiente. Además, tiene otras características como son:
 - Confidencialidad de la información.
 - Disponibilidad asegurada mediante una centralización lógica pero distribuida físicamente.
 - Ampliable y flexible en función de la información específica que se necesite.
 - Búsqueda mediante filtros con múltiples criterios.

Resuelve los problemas de NT, como son que NT no admite la creación de subdominios lo cual obliga a crear nuevos dominios, lo que multiplica el trabajo de administración ya que cada dominio

tiene su escala de usuarios y privilegios. Que un servidor sólo puede pertenecer a un solo dominio. Así como los problemas en la asignación de privilegios, ya que éstos se asignan en función del tipo de objeto y no del objeto en sí.

El directorio activo se basa en los siguientes conceptos:

- Dominio: es la estructura fundamental del directorio activo. Agrupa todos los objetos que se administran en una organización.
- Unidad organizativa: podemos dividir nuestro dominio en unidades administrativas más pequeñas y fáciles de manejar.
- Grupos: son conjuntos de objetos del mismo tipo.
- Objetos: son usuarios y recursos en general.

Las características principales de la nueva estructura son:

- Transitividad de las relaciones de confianza entre dominios.
- Multidominio, con lo cual un servidor puede albergar más de un dominio.
- Réplica multimaestro, que hará posible hacer modificaciones en el directorio en cualquier servidor y se actualizará en los restantes servidores del dominio.
- Podrá manejar más de 40.000 objetos en un único dominio.
- La administración de privilegios será mucho más flexible, seleccionando los conjuntos y subconjuntos de objetos a la hora de dar privilegios.
- Soporte de herencia en la administración de privilegios, lo cual hará que se propaguen de forma automática por el árbol de directorios a todos los niveles dependientes del mismo.

En resumen, en el directorio activo quedará unificada y centralizada de forma lógica mucha información que actualmente está desperdigada por múltiples lugares.

c) Administración.

La administración se realiza desde el programa MMC (Microsoft Management Console). Está dividido en tres partes: herramientas del sistema, almacenamiento y servicios y aplicaciones de servidor.

Permite la configuración de usuarios y de grupos y la definición de políticas del sistema. También se pueden usar políticas para implementar, actualizar o desinstalar aplicaciones a través de una red.

Las políticas de acceso definen las condiciones necesarias para el acceso y dependiendo de su cumplimiento o no se le garantiza o se le deniega el acceso, registrando todos los accesos en un archivo log, tanto los fallidos como los acertados.

En los puestos de usuario reduce el desorden en el escritorio y simplifica el menú de Inicio. Además elimina los objetos de escritorio innecesarios, presenta la posibilidad de configurar menús Personalizados, usando un dispositivo «inteligente» que adapta el menú de Inicio al modo de trabajo, mostrando aquellas aplicaciones que usa más a menudo.

d) Sistema de Almacenamiento.

El Distributed File System (Dfs) permite crear volúmenes virtuales que pueden residir en el mismo disco duro de un único servidor hasta estar repartidos en varios discos de distintos ordenadores.

El Dfs se puede organizar en función de las necesidades de cada momento, como puede ser un mejor rendimiento, aumentando la velocidad de respuesta o conseguir una mayor seguridad con la obtenida por la redundancia que se consigue replicando directorios, lo que permitirá a los usuarios seguir trabajando y accediendo a la información aunque un disco o un servidor dejen de funcionar. El sistema de archivos NTFS permite la encriptación de contenidos y la asignación de cuotas de disco a usuarios.

e) Comunicaciones.

Windows 2000, al igual que NT, puede hacer de router sobre los protocolos TCP/IP, IPX y además NAT, DHCP, IGMP, OSPF y RIP2. De ellos destaca IGMP, que permite ser configurado como proxy en lugar de router.

Además existe un nuevo servicio denominado Point of Presence (POP) que genera una lista de teléfonos a los que nuestros clientes llaman para conectar a nuestra red o de usuario móviles.

f) Seguridad.

Windows 2000 ha sido construida para ser muy segura en todos los niveles. El componente de firma digital autentifica a los usuarios y controla sus accesos, creando una puerta de entrada virtual a través de la que todos los usuarios, recursos y aplicaciones deben pasar obligatoriamente para introducirse en el sistema. Este proceso le otorga un control completo sobre los accesos a su ordenador, lo que contribuye a aumentar la seguridad del sistema operativo. Esta seguridad puede ser a distintos niveles:

- Local. Protege la información del disco duro del ordenador. El Sistema de Encriptación de Archivos (EFS), parte del Sistema de Archivo Windows NT, encripta cada archivo con una clave generada aleatoriamente. Los procesos de encriptación y desencriptación son invisibles a nivel de usuario.
- Corporativa. Protege la intranet o red corporativa, soporta Kerberos, un protocolo de autenticación de redes estándar para proteger la información mediante seguimiento y verificación de las actividades de cada usuario de la red.
- Pública. Protege las conexiones de Internet de la compañía. El soporte para seguridad de clave pública, un protocolo de autenticación estándar usado en las redes públicas, evita que el correo electrónico sea visto o editado por otros usuarios, asegura que las aplicaciones y drivers provengan de fuentes conocidas, y protege el software de intrusiones y actos de piratería una vez instalado.

K) LINUX.

La versión de Unix para ordenadores personales nace entre los años 1977-1982 cuando los laboratorios Bell recopilan todas las variantes que se habían producido dentro de AT&T en un solo sistema, al que se conoce comercialmente como XENIX SYSTEM III. Su principal inconveniente fue el hardware en el que se incorporaba. Unas máquinas basadas en microprocesadores de Intel 8086 y 8088, que sólo rodaban a 4,77 Mhz, y cuyos discos contaban con poca capacidad de almacenamiento y tiempos de acceso largos.

Una variante de este sistema operativo es el denominado LINUX, que en un principio sólo fue un proyecto de aficionado de Linux Trovalds pero en la actualidad se ha convertido en uno de los sistemas operativos mejor diseñados del mundo.

Éste es un sistema de libre distribución donde cualquier persona puede participar en la escritura del código. Esto lo hace todavía más interesante porque todos los programas fuente del sistema se pueden consultar y ver. En lo referente a la arquitectura el sistema Linux en la actualidad es un clónico de Unix capaz de ejecutar el entorno gráfico X-windows, TCP/IP y software de correo y News.

Linux es un sistema operativo completo multitarea y multiusuario como cualquier sistema Unix. Al ser un sistema operativo clónico de Unix, los conceptos sobre procesos y archivos son iguales que él. En Linux los dispositivos hardware son tratados como archivos y los software como procesos. Linux es un sistema operativo capaz de soportar redes y entornos gráficos si bien el entorno gráfico no forma parte del sistema operativo y se puede tener Linux en perfecto funcionamiento sin X-windows.

En cuanto a la comunicación, se realiza mediante tubos, de esta forma los procesos pueden pasarse información, estos tubos son ficheros intermedios y por tanto para leer y escribir en ellos se utilizarán las llamadas al sistema que permiten leer y escribir en ficheros.

Relacionado con esto de los permisos tenemos un conjunto de llamadas al sistema que nos permite cambiar los modos de los archivos, así como saber qué usuario pide una operación sobre un archivo para saber si éste tiene permiso para realizar la operación pedida o no.

Junto con las llamadas al sistema de gestión del sistema de ficheros tenemos también una serie de llamadas para la gestión de directorios, estas llamadas entre otras cosas nos permiten crear enlaces con ficheros así como montar sistemas de directorios.

Linux es capaz de ejecutarse en modo gráfico utilizando las X-Windows, las X no forman parte de SO en sí, pero proporcionan una interfaz gráfica para el usuario. El modelo que utiliza las X es el modelo cliente servidor, en el que procesos clientes (aplicaciones) realizan una serie de peticiones a procesos servidores que se encargan de ejecutarlas y dar respuesta a los clientes. Además de esto, Linux es un sistema operativo que incorpora soporte para redes y por tanto existen llamadas para gestionar esta red. De esta forma Linux se convierte en uno de los sistemas operativos con un diseño muy robusto y estable que proporciona un amplio soporte.

Linux es un sistema operativo que permite la multitarea o multiprogramación, es por esto por lo que en el núcleo existe una función que se encarga de la organización de los procesos. En el transcurso de la ejecución un proceso en Linux puede pasar por cinco estados diferentes. Estos estados son:

- En ejecución: el proceso es ejecutado por el procesador.
- A punto: el proceso podría ser ejecutado pero otro proceso se está ejecutando en ese momento.
- Suspendido: el proceso está en espera de un recurso.
- Parado: el proceso ha sido suspendido por una intervención externa.
- Zombi: el proceso ha terminado su ejecución pero sigue siendo referenciado en el sistema.

Los atributos que el sistema mantiene mientras un proceso se está ejecutando son: el estado, el valor de los registros, la identidad del usuario bajo cuyo nombre se ejecuta, las informaciones utilizadas por el núcleo para proceder al ordenamiento de los procesos (prioridad), las informaciones respecto del espacio de direccionamiento del proceso (segmentos de código, de datos, de pila), las informaciones respecto a las entradas/salidas efectuadas por el proceso y las informaciones que resumen los recursos utilizados por el proceso.

La forma que posee Linux para ejecutar varios procesos es muy parecida a la que poseen los demás sistemas operativos que admiten la multiprogramación. El sistema mantiene una lista de procesos a punto que podría ejecutar y procede periódicamente a su ordenamiento. A cada proceso se le atribuye un lapso de tiempo. Linux elige un proceso a ejecutar, y le deja ejecutarse durante ese lapso. Cuando ha transcurrido, el sistema hace pasar al proceso actual al estado a punto, y elige otro proceso que ejecuta durante otro lapso. El lapso de tiempo es muy corto y el usuario tiene la impresión de que varios procesos se ejecutan simultáneamente.

La función del núcleo que decide qué proceso debe ser ejecutado por el procesador es el Coordinador. Éste explora la lista de procesos a punto y utiliza varios criterios para elegir el proceso a ejecutar. El coordinador de Linux proporciona tres políticas de coordinación diferentes: una para los procesos «normales» y dos para los procesos de «tiempo real».

En Linux la gestión de memoria va a correr a cargo del núcleo. Utiliza la memoria paginada y el intercambio, además de la segmentación. La razón por la cual se utiliza este modo de gestión de memoria más complejo, que a su vez es también más completo, es para poder ejecutar, entre otras muchas cosas, el entorno gráfico Xwindows, además de dar soporte a la multiprogramación y multiusuario. Si unimos todo esto es fácil pensar que los programas a ejecutar pueden ser mayores que el tamaño de la memoria y que debido a tener soporte multiusuario los procesos en ejecución pueden ser muchos. Para realizar el intercambio Linux no sólo lo hará con el disco duro sino que como veremos más adelante será capaz de gestionar unos dispositivos llamados swap que no tienen por qué ser el disco duro.

Linux utiliza la segmentación para separar las zonas de memoria asignadas al núcleo y a los procesos. Dos segmentos se refieren a los tres primeros Gigabytes de espacio de direccionamiento de los procesos y su contenido puede leerse y modificarse en modo usuario. Los segmentos cuando entramos en modo núcleo se refieren al cuarto Gigabyte del espacio de direccionamiento y su contenido sólo puede leerse y modificarse en modo núcleo. De esta forma el código y los datos del núcleo quedan totalmente protegidos.

Linux utiliza los mecanismos de memoria virtual proporcionados por el procesador sobre el que se ejecuta. Las direcciones manipuladas por el núcleo y los procesos son direcciones virtuales y el procesador efectúa una conversión para transformar una dirección virtual en dirección física en memoria central.

Cuando varios procesos acceden a los mismos datos, Linux intenta compartir al máximo las páginas. Por ejemplo, si varios procesos ejecutan el mismo programa, el código del programa se carga una sola vez en memoria, y las entradas de las tablas de páginas de los diferentes procesos apuntan a las mismas páginas de memoria.

Bajo Linux, todo dispositivo en modo bloque o archivo regular puede usarse como dispositivo de swap. El núcleo de Linux guarda en memoria una lista de dispositivos de swap activos. Se utiliza una tabla de descriptores, en la que cada uno describe un dispositivo de swap.

Como hemos visto, Linux realiza una gestión de la memoria eficaz y totalmente independiente del procesador sobre el que se esté ejecutando.

La gestión de archivos en Linux va a ser realizada por el núcleo del sistema. Debido a que la gestión del sistema de archivos es realizada por el núcleo la comunicación entre los procesos y este núcleo se va a realizar mediante el uso general de las llamadas al sistema.

Los sistemas de archivos nativos de Linux reciben el nombre de ext2 y están formados por un bloque de autoarranque, que se ejecuta cuando se enciende la máquina, seguido de unos bloques para los nodos-i y finalmente los bloques de disco para el almacenamiento de los ficheros.

Cuando un proceso llama a una primitiva del sistema pasándole un nombre de archivo, el núcleo convierte el nombre especificado en un descriptor de archivo. Para ello, Linux explora cada uno de los directorios contenidos en la ruta del nombre y compara cada entrada de directorio con el nombre simple del elemento siguiente. Así hasta llegar al nodo-i que contiene la información del archivo que queremos abrir.

Una vez tenemos el archivo abierto es muy sencillo acceder a los diferentes bloque de datos del fichero ya que en el nodo-i del fichero se encuentran las direcciones de estos bloques.

Este sistema operativo es uno de los más completos que existe. Tiene la capacidad de gestionar sistemas de archivos que no son nativos de Linux (recordemos ext2).

La gestión de los distintos sistemas de archivos es posible gracias a una capa lógica que posee el núcleo cuya misión es asegurar la interfaz entre las llamadas al sistema respecto a los archivos y el código de gestión de archivos propiamente dicho. Esta capa recibe el nombre de sistema virtual de archivos (SVA).

Linux mantiene una lista de memorias intermedias en curso de utilización. Al realizar una lectura de bloque un sistema de archivo, el contenido del bloque se guarda en una memoria intermedia, llamada búfer. Esta memoria se guarda mientras el bloque está en curso de utilización, y mientras el espacio de memoria que ocupa no se necesita para otro búfer. Al realizarse una modificación de datos en un bloque, el cambio se efectúa en el contenido del búfer, que se marca como modificado pero no se escribe en disco inmediatamente. A intervalos regulares, el proceso update llama a la primitiva sync para forzar la reescritura de todos los búfers modificados.

- Seguridad.

Linux es un sistema pensado para la utilización en entornos multiusuario y por tanto el tema de la seguridad debe ser tratado cuidadosamente. La privacidad de datos y la consistencia de los mismos se aseguran en Linux mediante una serie de permisos que se le dan a los diferentes archivos.

A cada archivo se le asocian varios atributos:

- Su tamaño en bytes.
- El identificador del propietario del archivo.
- El identificador del grupo de usuarios del propietario.
- El número de enlaces que tiene.
- Sus derechos de acceso.
- Las fechas de acceso y modificación.

A nosotros nos interesan sus derechos de acceso. Éstos son los que se van a encargar de la seguridad.

Los derechos de acceso se expresan en una tripleta: los permisos del propietario, los permisos del grupo y los permisos del resto de usuarios. Cada uno de estos permisos está formado por tres derechos:

- El derecho a leer los datos del archivo «r».
- El derecho a escribir datos en el archivo «w».
- El derecho a ejecutar el contenido del archivo «x».

Gracias a la capa SVA, que contiene el núcleo, este sistema permite no sólo trabajar con sistemas de archivos nativos de él sino con otros que no tienen nada que ver. Esto, como se puede imaginar es un gran avance ya que se puede acceder a datos que están en otras unidades que no tienen por qué estar en formato Linux.

En el tema de la gestión de los dispositivos de almacenamiento es igual que en el sistema del que proviene, Unix, y como hemos podido observar es de gran sencillez gracias a la utilización de los nodos-i.

El tema de la seguridad también queda resuelto con el sistema de permisos descrito.

Todas estas razones, junto con las que hemos estudiado en los apartados anteriores, hacen pensar que este sistema operativo es uno de los más potentes que existen en la actualidad y que dará mucho que hablar en un futuro no muy lejano.



