APUNTES SOBRE REDES, tomado de
https://www.monografias.com/trabajos11/inter/inter.shtml el 03/03/2021

Indice

1. ¿Qué es la interconexión de redes?

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.
El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.
Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.
Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Tipos de Interconexión de redes
Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (RAL con RAL)

Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN)

- Interconexión de Área Extensa (RAL con MAN y RAL con WAN)

La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN)

2. Dispositivos de interconexion de redes.

Concentradores (Hubs)
El término concentrador o hub describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Se suele aplicar a concentradores Ethernet, Token Ring, y FDDI(Fiber Distributed Data Interface) soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y TokenRing).
Los primeros hubs o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica), y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.
Los hubs inteligentes de "segunda generación" basan su potencial en las posibilidades de

gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un período mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.
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, TokenRing, 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 hub) 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.

A un hub TokenRing se le denomina Unidad de Acceso Multiestación (MAU) Multiestation Access Unit). Las MAUs se diferencian de los hubs Ethernet porque las primeras repiten la señal de datos únicamente a la siguiente estación en el anillo y no a todos los nodos conectados a ella como hace un hub Ethernet. Las MAUs pasivas no tienen inteligencia, son simplemente retransmisores. Las MAUs activas no sólo repiten la señal, además la amplifican y regeneran. Las MAUs inteligentes detectan errores y activan procedimientos para recuperarse de ellos.

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. De esta forma se puede extender, teóricamente, la longitud de la red hasta el infinito.
Un repetidor interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI. Por esto sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico.
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 pueden clasificar en dos tipos:

- Locales: cuando enlazan redes próximas.

Remotos: cuando las redes están alejadas y se necesita un medio intermedio de comunicación.
En la siguiente figura se muestra un ejemplo de utilización de un repetidor.
Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red, no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que limita la distancia máxima entre los nodos más lejanos de la red a 1.500 m. (enlazando con dos repetidores tres segmentos de máxima

longitud, 500 m).
Ventajas:

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

Desventajas:

- Incrementa la carga en los segmentos que interconecta.

Los repetidores son utilizados para interconectar RALs que estén muy próximas, cuando se quiere una extensión física de la red. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), ThickEthernet (10Base5), ThinEthernet (10Base2), TokenRing, fibra óptica, etc.

Puentes (Bridges)
Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red.
Operan en el Nivel de Enlace del modelo de referencia OSI, en el nivel de trama MAC (Medium Access Control, Control de Acceso al Medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos en los dos niveles inferiores OSI, (como es TokenRing con TokenRing, Ethernet con Ethernet, etc) y conexiones a redes de área extensa.
Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas.
Las redes conectadas a través de bridge aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.
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 bridge:

- 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 Arbol 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 TokenRing.

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

Este tipo de bridges pueden 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.

Encaminadores (Routers)
Son dispositivos inteligentes que trabajan en el Nivel de Red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.
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
- 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 autentificación 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 Brouter, hacen de estos 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.

Pasarelas (Gateways)
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.

Conmutadores (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. Tendencias tecnológicas y del mercado

Las principales tendencias del mercado de sistemas de interconexión de redes son las siguientes:

- Tendencias de encaminamiento

El mercado está en expansión, cada vez hay más ofertas de productos y además estos incorporan nuevas facilidades de encaminamiento. Tanto los fabricantes de concentradores como los de multiplexores están incorporando en sus productos capacidades de encaminamiento, unos con redes de área metropolitana y extensa, y otros incorporando facilidades de interconexión de RALs.

- Equipos de interconexión a bajo coste

Los fabricantes están presentando equipos de bajo coste que permiten la interconexión de dependencias remotas. Las soluciones de encaminamiento son de diversos tipos: integradas en servidores de red, en concentradores, en pequeños equipos router, etc. Todos estos productos son fáciles de gestionar, operar y mantener.

- Routers multiprotocolo

Estos dispositivos han permitido a los usuarios transportar protocolos diferentes sobre la misma infraestructura de red, lo cual permitiría ahorrar en costes de la infraestructura de transmisión y una potencial mejora de la interoperabilidad.

- Interconexión de LAN/WAN bajo Switchers

Los conmutadores han evolucionado rápidamente dotándose de altas capacidades y velocidad de proceso. Pensados para soportar conmutación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) bajo una arquitectura punto a punto, han logrado gran implantación como mecanismo de interconexión de redes de área local heterogéneas, Token Ring y Ethernet en un mismo dominio. Esto se consigue dado que el conmutador permite la segmentación de la red en subredes conectadas a cada uno de sus puertos que puede gestionar de manera independiente.

- Capacidad de gestión

Los fabricantes están dotando a sus dispositivos de interconexión con mayores capacidades de gestión que permitan la monitorización de la red mediante estaciones de gestión y control de los dispositivos de la red, enviando comandos por la red desde la estación de gestión hasta el dispositivo de la red para cambiar/inicializar su configuración.

Análisis de las necesidades del comprador
Las razones para proceder a la adquisición de sistemas de interconexión de redes pueden estar determinadas por diferentes factores. Es labor del responsable de compras la realización de un análisis de necesidades existentes dentro de su organización que permita determinar las necesidades actuales y futuras de los usuarios y las limitaciones o restricciones que ha de plantearse respecto al dimensionamiento de la red y de los dispositivos de interconexión. Es necesario tener en cuenta y analizar en profundidad los costes y beneficios asociados para obtener argumentos de peso en la toma de decisiones.
En la fase de análisis de necesidades, fase inicial del proceso de adquisición, hay que tener en cuenta todos aquellos requisitos, limitaciones y restricciones que afecten, entre otros, a los siguientes puntos:

- Ventajas de la interconexión de redes

Hay que determinar si algunas de las ventajas que proporciona la interconexión de redes es aplicable a las necesidades de la organización. La interconexión de redes proporcionan diferentes ventajas:

- Compartición de recursos dispersos o de otras redes.
- Extensión de la red y aumento de la cobertura geográfica.
- Segmentación de una red.
- Separación entre redes.
- Conversión de protocolos.

Antes de segmentar una red es recomendable realizar un estudio de flujos de datos, porque puede suceder que al realizar la partición en segmentos se aumente el tráfico en los segmentos en vez de disminuirlo.

- Número de redes que van a ser conectadas y topología de las redes

El conocimiento del número de redes a interconectar y las características específicas de cada uno de ellas, permitirá dimensionar correctamente tanto la estructura de la red final como los elementos necesarios para realizar la interconexión.
También se han de analizar las necesidades de adquisición de nuevas redes o infraestructura de red para poder dar soporte a la futura red.
Es necesario delimitar claramente el tipo de redes existentes (Ethernet, TokenRing, FDDI, etc), su topología (estrella, bus, anillo, etc), su distribución espacial en el entorno de operación (localización y distancias). Es recomendable realizar planos del entorno en cuestión.

- Características del entorno físico de operación

La interconexión de redes exige por lo general el tendido de cableado en las dependencias por las que se extienden las redes y ello es una labor cuya complejidad, impacto y coste depende de varios factores. Entre éstos habrá que considerar el área cubierta por las redes y

por su interconexión (ubicaciones, departamentos y edificios a interconectar), sus topologías, las peculiaridades constructivas de los locales o edificios, y otras cuestiones que pueden afectar no sólo al coste sino incluso a la viabilidad de la implantación de la interconexión de redes.

- Estimación del coste de adquisición, operación y mantenimiento

El coste de adquisición de dispositivos de interconexión de red tiene varios componentes, directos e indirectos. Todos ellos han de ser tenidos en cuenta si se quiere realizar una previsión razonable de fondos. Los principales factores de coste son los siguientes:
Dispositivos físicos de la red: medio de transmisión, elementos de conexión de los nodos, etc.
Dispositivos lógicos de la red: sistemas de gestión, control y mantenimiento.
Instalación: acondicionamiento de locales, canalización, tendido de cables, conexión de dispositivos, etc.
Costes indirectos: redimensionamiento de nodos pasivos y activos, elementos complementarios, etc.
En ningún caso debe despreciarse a priori la importancia de ningún tipo de costes.
El responsable público de adquisición deberá de disponer de una estrategia de redes perfectamente elaborada para poder satisfacer las necesidades que se puedan plantear en un futuro. Cuando una red está instalada, ésta crece de forma continuada, aumentando en equipos anteriormente no considerados y llegando a lugares no contemplados, soportando nuevas aplicaciones..., lo cual demandará capacidades no imperativas inicialmente

Factores relevantes en el proceso de adquisición
En la definición del objeto del contrato y los requisitos inherentes al mismo, así como en la valoración y comparación de ofertas de los licitadores pueden intervenir muchos factores y de muy diversa índole.
Es de suma importancia que todos los factores relevantes que intervienen en el proceso de contratación queden debidamente recogidos en el pliego de prescripciones técnicas que regule el contrato. Así mismo, es conveniente que las soluciones ofertadas por los licitadores sean recogidas en los cuestionarios disponibles a tal efecto:
De empresa
Económicos
Técnicos particulares
No obstante y a título orientativo en este apartado se hace mención de aquellos factores, que entre los anteriores, pueden intervenir en el proceso de adquisición de equipos y sistemas de interconexión de redes y cuyo seguimiento debe efectuarse exhaustivamente:

- Número de puertas disponibles

Cuando se decide seleccionar un dispositivo de interconexión no sólo hay que tener en cuenta el número de puertas necesarias; hay que pensar en el crecimiento futuro. Interesa dejar un número de puertas disponibles para tener siempre capacidad de crecimiento. Es importante definir un tanto por ciento de puertas libres respecto a las utilizadas. Este porcentaje varía de una implantación a otra y normalmente está condicionado también por el coste de los dispositivos. Algunos de los dispositivos necesitan conexión remota o local de consola, por lo que habrá que tener en cuenta que el dispositivo presente esta característica.

- Gestión disponible

SNMP
CMIP
CMOT
La complejidad de las redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar las redes y los dispositivos de interconexión. Los routers son dispositivos que necesitan que se realicen funciones de gestión. En los otros dispositivos es recomendable que tengan esta facilidad.
Es conveniente analizar si la gestión del dispositivo ofertada es propietaria o es abierta,

tendiendo siempre a la última opción.
Pruebas de aceptación final
En función de los elementos técnicos que intervienen y del alcance abarcado, se definen distintos tipos de pruebas sobre los siguientes entornos de una red de datos:
1º) Operativa de Red:
Se distingue entre lo que es un funcionamiento normal de la red y el funcionamiento o reacción de ésta ante los diversos fallos que puedan producirse. Entendiendo por funcionamiento normal, aquél en el que los equipos y la red se encuentran en óptimas condiciones.

Funcionamiento normal.
Se realizarán las comprobaciones de las siguientes funcionalidades:

- Comunicaciones entre Puertos.
    -
    - Comprobar las comunicaciones a través de una red.
    - Comprobar las comunicaciones con redes externas.
    - Comprobar la existencia de derechos de acceso a los distintos puertos de las tarjetas de los diferentes equipos.
- Configuraciones dinámicas.
    -
    - Comprobar que las inserciones o extracciones de tarjetas de una red, no afectan al funcionamiento de la misma.
    - Comprobar que la extracción o inserción de una tarjeta router, no afecta al funcionamiento de las redes locales conectadas a ese router.
    - Comprobar que un cambio en la configuración de una tarjeta, no afecta al funcionamiento del resto de la red.

Funcionamiento ante fallos.
Se realizarán pruebas destinadas a la comprobación de cómo reacciona la red, en el caso de que se produzcan fallos en distintos elementos de la misma.

- Comprobar que las redes siguen funcionando aisladamente, después de la caída de un ramal.
- Comprobar el funcionamiento de las redes ante la caída de una tarjeta de un equipo.

2ª) Gestión de Red
Funcionamiento propio del sistema de gestión:

- Comprobar el funcionamiento de la red ante la caída del sistema de gestión.
- Comprobar que existe un control de accesos al sistema de gestión de red, con distintos niveles de seguridad.

Monitorización de la red.

- Comprobar que el sistema de monitorización gráfica responde en tiempo real a los eventos que ocurren en la red.
- Comprobar que se pueden visualizar distintos niveles dentro de la topología de la red.

Tratamiento de alarmas.

- Comprobar que el fallo, y posterior recuperación de elementos de la red, provoca las alarmas adecuadas.
- Comprobar la existencia de herramientas de prueba remota.
- Comprobar la existencia de distintos niveles de alarmas, y que pueden ser definidas por el usuario.

Informes y estadísticas.
Analizar con las herramientas disponibles la actividad de la red y la creación de informes sobre la misma.