El diseño de una LAN

Durante el diseño de la red solo deben preocuparte dos cosas:

- ?? las personas y
- ?? el desempeño.

Es Tú trabajo analizar el reporte de requerimientos y colocar los resultados por prioridad con respecto a las personas y el desempeño.

El diseño debes llevarlo a cabo en dos fases:

a) Diseño de una topología

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son :

- ?? La distribución de los equipos a interconectar.
- ?? El tipo de aplicaciones que se van a ejecutar.
- ?? La inversión que se quiere hacer.
- ?? El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- ?? El tráfico que va a soportar la red local.
- ?? La capacidad de expansión. Se debe diseñar una intranet teniendo en cuenta la escalabilidad.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

TOPOLOGÍA FÍSICA

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topología físicas puras :

- ?? Topología en anillo.
- ?? Topología en bus.
- ?? Topología en estrella.

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por mas de una topología física.

TOPOLOGÍA LÓGICA

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas :

- ?? Topología anillo-estrella : implementa un anillo a través de una estrella física.
- ?? Topología bus-estrella : implementa una topología en bus a través de una estrella física.

TOPOLOGÍA EN BUS

Consta de un único cable que se extiende de un ordenador al siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada **terminador,** que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus.

Sus principales ventajas son :

?? Fácil de instalar y mantener.

?? No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

Sus principales inconvenientes son :

?? Si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unirlas todas a través de un bus troncal.

TOPOLOGÍA EN ANILLO

Sus principales características son :

?? El cable forma un bucle cerrado formando un anillo.
?? Todos los ordenadores que forman parte de la red se conectan a ese anillo.
?? Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo "paso de testigo".

Los principales inconvenientes serían :

?? Si se rompe el cable que forma el anillo se paraliza toda la red.
?? Es difícil de instalar.
?? Requiere mantenimiento.

TOPOLOGÍA EN ESTRELLA

Sus principales características son :

?? Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.
?? Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio poolling, siendo el nodo central el que se encarga de implementarlo.
?? Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.
?? existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.
?? La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
?? Este tipo de topología se utiliza cuando el trasiego de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
?? Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
?? es fácil de detectar y de localizar un problema en la red.

TOPOLOGÍA EN ESTRELLA PASIVA

Se trata de una estrella en la que el punto central al que van conectados todos los nodos es un concentrador (hub) pasivo, es decir, se trata únicamente de un dispositivo con muchos puertos de entrada.

TOPOLOGÍA DE ESTRELLA ACTIVA

Se trata de una topología en estrella que utiliza como punto central un hub activo o bien un ordenador que hace las veces de servidor de red. En este caso, el hub activo se encarga de repetir y regenerar la señal transferida e incluso puede estar preparado para realizar estadísticas del rendimiento de la red. Cuando se utiliza un ordenador como nodo central, es éste el encargado de gestionar la red, y en este caso suele ser además del servidor de red, el servidor de archivos.

TOPOLOGÍAS LÓGICAS

TOPOLOGÍA ANILLO-ESTRELLA

Uno de los inconvenientes de la topología en anillo era que si el cable se rompía toda la red quedaba inoperativa; con la topología mixta anillo-estrella, éste y otros problemas quedan resueltos. Las principales características son :

- ?? Cuando se instala una configuración en anillo, el anillo se establece de forma lógica únicamente, ya que de forma física se utiliza una configuración en estrella.
- ?? Se utiliza un concentrador, o incluso un servidor de red (uno de los nodos de la red, aunque esto es el menor número de ocasiones) como dispositivo central, de esta forma, si se rompe algún cable sólo queda inoperativo el nodo que conectaba, y los demás pueden seguir funcionando.
- ?? El concentrador utilizado cuando se está utilizando esta topología se denomina MAU (Unidad de Acceso Multiestación), que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.
- ?? A simple vista, la red parece una estrella, aunque internamente funciona como un anillo.
- ?? Cuando la MAU detecta que un nodo se ha desconectado (por haberse roto el cable, por ejemplo), puentea su entrada y su salida para así cerrar el anillo.

TOPOLOGÍA BUS-ESTRELLA

Este tipo de topología es en realidad una estrella que funciona como si fuese en bus. Como punto central tiene un concentrador pasivo (hub) que implementa internamente el bus, y al que están conectados todos los ordenadores. La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

b) Diseño de modelos de nombramiento

La **denominación**, o gestión de nombres, es la correspondencia entre objetos lógicos y físicos. Por ejemplo, un usuario trata con conjuntos de datos representados por nombres de archivos, mientras que el sistema gestiona bloques físicos de datos almacenados en pistas de un disco. Normalmente el usuario se refiere a un archivo por un **nombre** textual, el cual posteriormente se traduce a un **identificador** numérico que acaba refiriéndose a bloques de un disco. Esta correspondencia entre los dos niveles proporciona a los usuarios una abstracción de cómo y dónde están realmente almacenados los datos.

Capacidad y estructura del esquema de nombres .
El Espacio de Nombres puede tener una **capacidad** *Limitada* o *Infinita*. El actual espacio de las direcciones de Internet es un ejemplo de capacidad limitada (ej. 138.100.56.34).

En cuanto a su **estructura**, puede ser *Plana* o *Jerárquica*. La estructura plana de nombres está asociada a espacios de nombres de capacidad finita (a no ser que la longitud de los nombres sea ilimitada), mientras que en la estructura jerárquica las direcciones pueden crecer indefinidamente. Cuando se utiliza la estructura jerárquica, se dice que la resolución de nombres se realiza de "acuerdo al contexto", es decir, traduciendo cada uno de los nombres anteriores al nombre final que indican la jerarquía por la que hay que pasar hasta llegar al objeto concreto.
Ejemplo: `mx.geocities.com/nancy_aguas/redes.html` hace referencia a un archivo (`redes.html`) situado en la máquina `geocities` en Mexico. Para resolver tales nombres se va ascendiendo por esta jerarquía de nombres, de tal forma que en cada nivel se es capaz de resolver el nombre y obtener la dirección del siguiente nivel hasta llegar a la máquina de destino, y en ella obtener el objeto con el nombre indicado (`redes.html`).No se debe confundir la capacidad de nombres con la capacidad de identificadores de dirección. Así, por ejemplo, aunque el actual sistema de direcciones de Internet es finito (en número de máquinas), el número de algunos recursos referenciables en la red es ilimitado, puesto que cada máquina puede contar con una estructura jerárquica de archivos potencialmente ilimitada (salvo por la capacidad y limitaciones de tablas).

Podemos ver, entonces, la necesidad de la resolución o traducción de nombres por identificadores de dirección. Una posibilidad sería que cada programa o sistema operativo de un sistema se programara directamente con las direcciones de todos los objetos actuales y futuros de la red completa, pero no resultaría muy práctico, pues no es fácil conocer, a priori, todos los posibles objetos de una red, y sería imposible realizar cualquier cambio de dirección. Parece mucho más razonable ver que esta resolución de nombres no es más que un nuevo servicio que debe ofrecer el sistema a los clientes.

Este nuevo servicio de resolución de nombres se denomina **Servidor de Nombres** (en inglés también se le conoce como *binder*, ya que a la traducción de nombres se le denomina *binding*). Así, cuando un cliente necesite conocer la dirección de cualquier servidor, lo único que tiene que hacer es preguntarselo al servidor de nombres. Desde luego, el servidor de nombres residirá en alguna de dirección bien conocida.

Funciones del Servidor de Nombres. Ya hemos visto que la función básica del servidor de nombres es la resolución o traducción de un nombre a un identificador, pero requiere otros servicios adicionales:

Resolución: La traducción del nombre por el identificador de comunicación.
Inclusión: Añadir una pareja nombre/identificador al servidor de nombres.
Borrado: Eliminar una entrada del servidor de nombres.
Modificación: Modificación del nombre/identificador de una entrada.

Ya hemos comentado que cuando un cliente requiere cualquier servicio del sistema, primero es necesario comunicarse con el servidor de nombres para obtener el identificador de un servidor del servicio requerido. ¡Y si el servidor de nombres falla o se cae? La respuesta es clara: Se pierden todos los servicios del sistema.

Dada la importancia del servidor de nombres, cuyo funcionamiento es vital para el resto del sistema, parece que se hace necesario que este servicio especial sea **tolerante a fallos**. Teniendo en cuenta, además, que va a ser un servicio muy requerido, pues todas las utilizaciones de cualquier servicio deben pasar primero por él, para facilitar la tolerancia a fallos y evitar el cuello de botella, suele ser normal que el servicio de nombres esté formado por servidores replicados que ofrezcan este servicio de nombres.

Para acceder a un objeto remoto, el proceso cliente (que sólo conoce el nombre del recurso) debe conseguir el identificador de comunicación del recurso que solicita antes de comunicarse realmente con él. Para ello debe acudir primero a los servidores de nombres intermedios necesarios hasta conseguir dicho identificador de comunicación, con el consiguiente tiempo de demora debido a los tiempos de resolución o traducción de cada uno de los servidores de nombres requeridos.
Cuando se está accediendo a menudo a un objeto remoto, para evitar el tiempo de resolución de los nombres intermedios, el proceso cliente puede mantener una **tabla caché** con los identificadores de dirección de los objetos más recientemente referenciados, y utilizar directamente estos identificadores para acceder a los objetos.

A la hora de diseñar un sistema de nombres o de denominación, se deben perseguir estos dos objetivos:

•**Transparencia de ubicación**. El nombre de un objeto no debe revelar su ubicación física.
•**Independencia de ubicación**. El nombre del objeto no debe cambiar cuando cambie su ubicación física. Esto implica transparencia dinámica, ya que un nombre puede asociar el mismo objeto a lugares diferentes en momentos distintos.
Actualmente, la mayoría de los sistemas proporcionan simplemente la transparencia de ubicación, por lo que no ofrecen ***migración***, es decir, el cambio **automático** de ubicación de un objeto sin afectar a sus usuarios o clientes. Chorus y Charlotte son ejemplos de sistemas que permiten la migración.

Nombres Puros e Impuros. Los nombres **puros** son simplemente series de bits sin ninguna interpretación posible (salvo para el servidor de nombres). Otros nombres (los impuros) incluyen bits que indican directamente una dirección, permisos de acceso o cualquier otra información sobre el objeto.

Los nombres **impuros** entran en conflicto con el principio de transparencia al que tanto hemos aludido. Obsérvese que con un nombre impuro, cualquier información implícita que lleve, puede quedarse obsoleta si el recurso al que se refiere cambia su dirección, permisos, etc. Con los nombres puros simplemente hay que preocuparse de mantener actualizadas las bases de datos de los servidores de nombres de cada contexto.

Control de acceso. Para evitar accesos no autorizados a los recursos del sistema, un primer paso consiste en hacer que el identificador de un recurso no se pueda obtener fácilmente a partir de su nombre si no es a través del servidor de nombres. Y, por supuesto, el servidor de nombres debe ocuparse de comprobar la identidad del cliente que solicita una resolución de nombres antes de darles el identificador solicitado. Los identificadores que se comportan así, se denominan **credenciales** *(capabilities)*. Por eso se dice que para poder acceder a un recurso o servicio, previamente debe obtenerse la credencial correspondiente.

Ejemplo: **Credencial de Amoeba**. Cuando un cliente requiere cierto servicio, en primer lugar se identifica y solicita la credencial correspondiente al servidor de nombres, el cual devuelve la credencial solicitada para el cliente identificado. Una vez se tiene la credencial, se obtiene de ella

el *Puerto* del servidor que va a prestar el servicio requerido, con lo que ya se le puede enviar el mensaje con la la petición del servicio y la credencial completa.
El campo *Objeto* lo utiliza el servidor para identificar el objeto específico con el que el cliente quiere realizar alguna operación. Para el caso de un archivo, este campo sería algo parecido a un inodo de Unix.

Los *Derechos* están compuestos por una serie de bits que indican las operaciones que le están permitidas al usuario para ese objeto (por ej. lectura, escritura, ...).
El campo *Verificación* se utiliza para dar validez a la credencial. La verificación la establece el servidor de nombres mediante un cierto algoritmo en función del resto de los campos de la credencial, y el servidor del objeto comprueba si la verificación que le llega efectivamente es la correspondiente a esa credencial. De ser así, y si cuenta con los derechos apropiados realiza la operación solicitada; en caso contrario, devolverá algún código de error al cliente.
De esta manera se evita que cualquier proceso de la red solicite indiscriminadamente cualquier operación, pues las credenciales solamente las pueden construir los servidores de nombres, y solamente mediante éstas puede solicitarse operaciones a los servidores.

c) Selección de protocolos de enrutamiento, conmutación y puenteo

Ver archivo anexo.

d) Desarrollo de estrategias de seguridad y gestion

La importancia de la seguridad depende de la función principal de la LAN. Debe empezar con un modelo de seguridad o estrategias basadas en políticas internas. Además de las funciones de seguridad del Sistema Operativo de Red, considere las fugas de información, intervenciones, identificación de usuarios, pistas de auditorías y encriptación de datos.

En la segunda fase de análisis y diseño, tomaremos en cuenta los componentes de Hardware, estos se dividen en cuatro categorías:
· Componentes de Topología (selección de tecnologías)
· Cableado
· Servidor / Estaciones de trabajo (selección de dispositivos de red)
· SFT

Componentes de topología. Incluye el hardware que conecta todas las máquinas entre si. Como Network Interface Cards (NICs), hubs, etc. El servidor de archivos establece los procedimientos de comunicación para las estaciones de la red y reserva recursos compartidos de la red. El servidor de archivos también contiene el sistema operativo de la red. Las estaciones de trabajo realizan el 95% de la carga de procesamiento de la red.

También, cada estación representa el enlace entre el usuario y la LAN. Finalmente, SFT, el componente de la red más pasado por alto, aún cuando SFT representa la única protección de la red en contra de corrupción de datos, sobrecargas de voltaje, perdida de datos y en general, las caídas de la red.

Componentes de Topología

La primer decisión de diseño orientada al hardware es como configurar fisicamente los componentes de la red. Debemos considerar muchos factores para desarrollar la mejor formula para eficiencia, desempeño, y Habilidad.

Afortunadamente, el 95% del mundo de redes se ha basado en una de 4 topologías:

Thin Net (Red delgada en canal) o Bus también Ethernet 10BASE2
Thick Net (Red Gruesa en canal) o Bus también Ethernet 10BASE5
Star o Estrella también Ethernet 10Base-T
Token Ring o Anillo

Estos estandares combinan dos conceptos críticos de hardware:
Topología y Protocolo. La Topología describe la distribución geográfica de los componentes de la red. EI protocolo es el juego de reglas que controlan la comunicación a traves de la red. La topología y el protocolo se combinan para crear un estandar de red eficiente. Cada uno de los cuatro estandares de red tiene sus ventajas y desventajas. Es tu trabajo durante el diseño de la red balancear las necesidades de la red con alguno de los estandares.
Ethernet, por ejemplo, es rápido, barato, y fácil de entender. EI problema es, en algunos casos que no es muy confiable. Token ring es mas confiable y hasta un poco mas rápido. Pero, Token Ring es más caro.

Cableado

Las redes utilizan el cable para conectividad, confiabilidad y velocidad. En el pasado, el tipo de cable que seleccionabas se basaba en la topología: Ethernet 10Base2 usaba coaxial RG58, mientras que Token Ring usaba STP (shield twisted pair). Hoy, la industria es lo suficiente flexible que cualquier topología puede correr en casi cualquier tipo de cable, La industria utiliza como estandares para LAN´s Unshielded Twisted Pair (UTP), Shielded Twisted Pair (STP), Coaxial RG58, y la Fibra Óptica.

Servidor / Estaciones de trabajo

La meta de todo esto es conectar computadoras. Estas computadoras incluyen servidores de archivos y estaciones de trabajo. El servidor de archivos tiene un impacto muy grande en el desempeño de la red. Contiene el Sistema Operativo de la Red, procesa peticiones del disco, almacena aplicaciones de red
y datos, controla la seguridad de la red, entre otras importantes funciones.
Sin embargo, la función principal del servidor de archívos es “Procesar Peticiones de la LAN aceptando data packets y mandándolos a procesos internos”.
La función principal de la estación de trabajo es procesamiento de datos y servir de interfase entre el usuario y la red.

System Fault Tolerance SFT
SFT es una medida de que tan tolerante es el sistema a fallas. Un nivel alto de SFT significa que la LAN puede soportar caidas de disco duros, sobrecargas de voltajes, corrupción de datos y posiblemente evitar una perdida total de datos.

Existen dos tipos de fallas del sistema: Fallas de voltaje y perdida
de datos.

Fallas de voltaje ocurre cuando tenemos sobrecargas o cuando no hay voltaje. Fallas de voltaje pueden ocasionar caidas del servidor y corrupción de datos.

La pérdida de datos es frecuentemente atribuida a fallas de disco del servidor. La Pérdida de datos también puede ocurrir cuando los usuarios borran archivos, existen datos corruptos o se introduce un virus destructivo a la red. Es necesario para el diseño de hardware, que incorpores multiples niveles de SFT.

Algunos componentes incluyen Fuente ininterrupibles de voltaje (UPS´s), espejeo/duplexing de discos y algunas características de Seguridad.

Diseño de Software

La fase final del Análisis y Diseño de una Red, trata con el software de la LAN. El software de la LAN describe los componentes que no puedes tocar.

Provee al sistema de productividad, interfase con el usuario, administración del sistema y lo más importante conectividad transparente. El software de la LAN consiste de cuatro componentes:

· Sistema Operativo de la Red (NOS) [Network Operating System]
· Sistema Operativo de las Estaciones de Trabajo
· Software de Conectividad
· Software de Menú/Aplicación (Paqueterías, Utilerías)

El NOS es el corazón de la LAN. Reside en el servidor de archivos central y controla operaciones críticas de la red como peticiones de archivos, routing de packets, seguridad de la red, interconectividad, y administración del sistema.

El Sistema Operativo de la Estaciones de Trabajo (WOS) reside en estaciones distribuidas y se encargan de procesamiento local y colocación de recursos. La conexión clave entre las estaciones y el sistema operativo de la red es proveída
por el software de conectividad que son los drivers, y en general todo aquel software que le dan posibilidad de comunicación y enlace a nuestra estación de trabajo.

Finalmente, las aplicaciones y sistemas de menú proveen de funcionalidad al usuario. La Paquetería o utilerías son herramientas de productividad que le agregan valor a la red. Estas herramientas crean e interoperan los comandos que van de computadora a computadora. Los menús proveen a la LAN con una interfase amistosa y productiva al usuario. Estos sistemas integran aplicaciones de la red, dirigen funciones de la LAN y monitorean constantemente la utilización de recursos. Sin aplicaciones/menús, la LAN no sería otra cosa que un “tiovivo electronico”. Veamos un poco mas de estos componentes críticos y exploremos como impactan el análisis y diseño del software.

Sistema Operativo de la Red (NOS)

El cerebro de la LAN se encuentra en el NOS. El NOS cae en una de dos categorias:

· Cliente/Servidor
· Punto a Punto

En redes de cliente/Servidor, el NOS reside en un nodo central
controlador -El servidor de archivos-. En redes de Punto a Punto los nodos distribuidos comparten la carga de administración de la red y la asignación de recursos. Discos duros locales se convierten en disco de la red y las impresoras distribuidas se unen como un solo recurso. La mayoría de la LAN´s utilizan un Sistema Operativo cliente/servidor porque estos proveen una mejor seguridad, una administración más flexible y un mejor desempeño. Aproximadamente el 70% de todos los NOS son cliente/servidor.

Sistema Operativo de Estaciones de Trabajo (WOS)

Si el “caballo de trabajo” de la LAN es el Sistema Operativo, las riendas las lleva el WOS (Workstation Operating System).
El WOS administra el procesamiento local y los recursos de la estación mientras mantiene una conexión estable a la LAN. La belleza de algunos sistemas operativos de red es que soportan varios sistemas: DOS, OS/2, Windows NT, UNIX y Macintosh System 7 por ejemplo. El WOS reside en la estación y maneja los requerimientos de procesamiento para comunicaciones de las Máquinas, funciones locales de la computadora y aplicaciones distribuidas de la red. Además, el WOS define la interfase del usuario. Esta es la función mas importante junto con la interoperabilidad.

Software de Conectividad

Cada estrategia de conectividad es responsable de las comunicaciones de protocolo de la NIC y de redirecciones de DOS. Novell Network, por ejemplo, provee una solución de conectividad para cada uno de los WOS´s: ODI/VLM para DOS, OS/2 Requester para OS2, NT Requester para Windows NT, Chooser/Netware para Macintosh System 7 y Netware for NFS para UNIX. Tu responsabilidad principal durante el diseño de software es asegurarte que exista una solución de conectividad para cada unos de los WOS´s de tus usuarios.

Sistemas de Aplicaciones/Menús
Si el WOS controla el ambiente de la estación; las aplicaciones y menús le dan un propósito. Como habíamos mencionado, las aplicaciones son herramientas de productividad que le agregan valor a la LAN. La mezcla adecuada de aplicaciones puede salvar miles de dólares al incrementar la productividad y eficiencia.

Existen dos tipos de aplicaciones: Standalone y Netware aplications: Software Standalone son aplicaciones que no son hechas para corre en la LAN.
Estas aplicaciones pueden sin embargo operar en el servidor pero su capacidad de compartir archivos esta severamente limitada.

Aplicaciones Compatibles o de tipo Netware, son mas complejas porque son diseñadas para tomar ventaja del sistema multiusuario de la red. Funciones adicionales incluyen seguridad en aplicaciones, compartir archivos, loocking de archivos, ahorro de costos y eficiencia de almacenamiento. Sin importar cual sea la función de la LAN, los usuarios deben sentirse agusto usandola. Esta es la responsabilidad del sistema. La meta del menú es proveer acceso sencillo e intuitivo a los servicios y aplicaciones de la red. El menú usualmente representa el primer contacto del usuario con la red y tiene un impacto psicológico considerable en la aceptación/rechazo de la LAN. Asegurate de realizar cuidadosamente la selección de un sistema de menú.

El diseño y análisis de una red intenta proponer algunas opciones. Estas opciones de diseño forman la funcionalidad y fuerza de tu LAN para siempre. Se paciente, pasa el tiempo suficiente y toma gran cuidado en que diseño de la LAN se adapte a las necesidades y requerimientos del sistema.