

# INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE LOS CABOS



*“Por una patria con sabiduría y espíritu de progreso”*

**Nombre del proyecto:**

Resumen de administración y gestión de una LAN

**ASIGNATURA:**

Administración de redes

**CARRERA:**

Ing. En Sistemas Computacionales

**ALUMNO(A):**

José Luis Hernández Mendieta

**GRUPO:**

8IS-01M

**DOCENTE:**

M.S.C. Xochitl Yadira Cota Luna

San José del Cabo B.C.S.

11 de Febrero del 2018

En esta lectura de administración y configuración de una red LAN pudimos apreciar que la persona encargada de las tareas de administración y seguridad en los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global, es el administrador de red. Este conjunto abarca tanto a servidores como a las estaciones clientes, el hardware y el software de la red, los servicios de red, las cuentas de usuario, las relaciones de la red con el exterior, etcétera.

Algunas de estas tareas han sido previamente explicadas: configuración de protocolos, instalación del NOS, diseño e implementación del cableado, etc. No obstante, aparecen funciones nuevas que se apoyan en las anteriormente citadas y que estudiaremos a continuación.

En ocasiones, estos conocimientos sólo se pueden adquirir en los departamentos de formación de las compañías suministradoras del hardware y software de las redes o entidades similares. El trabajo propio de mantenimiento puede ser realizado por miembros de la propia empresa, o bien contratar estos servicios con terceras empresas.

Corresponde al administrador de la red, como tarea especialmente importante, la decisión de planificar qué ordenadores tendrán la función de servidores y cuáles la de estaciones clientes, de acuerdo con las necesidades existentes en cada departamento u organización.

Del mismo modo, se ocupará de las relaciones con otros departamentos, grupos o dominios de red, en lo que se refiere a la utilización de los recursos de otros grupos, así como de la comunicación entre los diferentes dominios de gestión.

### Servidores de la red

Cuando se establece una estrategia de red es importante, en primer lugar, realizar una buena elección de los servidores con los que se contará. El número y prestaciones de los servidores de red están en función de las necesidades de acceso, velocidad de respuesta, volumen de datos y seguridad en una organización.

El número de servidores determina en gran medida la configuración de la red. Efectivamente, si sólo disponemos de un único servidor, éste debe ser compartido por toda la organización. Sin embargo, si se dispone de varios servidores cabe la posibilidad de arbitrar distintas configuraciones.

A pesar de que la carga de trabajo en una organización no exija más de un servidor, puede ser recomendable la existencia de varios servidores, por razones de seguridad, de reparto de flujo de datos, de localización geográfica, etcétera.

Cuanto mayor es el número de servidores de una red, mayor es la carga administrativa, incrementándose también los costes de mantenimiento. Por tanto, en una red no debe haber más servidores que los necesarios.

También hay que asegurarse de que si una aplicación tiene previsto utilizar un interfaz de aplicaciones concreto, por ejemplo, NetBIOS, debe estar instalado, ya que de lo contrario la aplicación de usuario no podrá gestionar las unidades de red remotas. Éste sería el trabajo típico de un redirector, como ya se veía en la Unidad anterior.

Los programas y aplicaciones están instalados en el disco duro local de la estación y no son compartidos por la red. Cada usuario tiene una copia de cada aplicación. Los datos residen también de modo habitual en el disco local, aunque es posible centralizar la información en los servidores.

La clasificación anterior está muy simplificada. La realidad es mucho más compleja. Lo habitual en el mundo de los sistemas de red son combinaciones de todas estas posibilidades y, por ejemplo, máquinas que son servidoras con respecto de un tipo de servicio son clientes con respecto de otros.

De la eficacia al diseñar esta estructura de red depende el éxito del administrador de red dando un buen servicio a los usuarios de la red que administra.

El acceso de un usuario remoto puede ser similar al acceso de un usuario local, disponiendo de los mismos servicios, aunque con rendimientos menores, debido a la inferior capacidad de transferencia de las líneas de transmisión de las redes WAN utilizadas en la conexión. Para ello, basta con disponer de los servicios de conexión y validación apropiados. Éste es el fundamento del teletrabajo.

#### Conexiones externas a la red

Además de los clientes y servidores de la red, es común la comunicación de datos entre la red de área local y el exterior, ya sea con usuarios de la misma o de distinta organización, pertenecientes o no a la misma red corporativa

#### El sistema de acceso a la red

Los programas están instalados en el servidor y todos los usuarios acceden al servidor para disparar sus aplicaciones. Por tanto, se instala una única copia de las aplicaciones, lo que ahorra espacio en disco. Hay que tener en cuenta, no obstante, que no todas las aplicaciones permiten esta operativa de trabajo. Los datos de usuario pueden seguir estando distribuidos por las estaciones clientes, aunque también pueden residir en el servidor.

## Estaciones clientes

En las estaciones de trabajo se han de instalar y configurar todos los protocolos necesarios para la conexión a cuantos servidores necesiten los usuarios.

El acceso a la red es el primer aspecto en que debemos fijarnos una vez instalado el software de red. Los servicios que ofrece una estación conectada a la red pueden ser utilizados por cualquier usuario que utilice esa estación de trabajo.

El orden y la confidencialidad de cada puesto de trabajo o proyecto requieren un sistema que garantice que cada persona tenga acceso a sus datos y aplicaciones, evitando que otros usuarios puedan ser perjudicados por el uso indebido del sistema o por la falta de una intención recta.

Cualquier administrador de sistema o de red tiene que tener en cuenta el posible asalto a la red por parte de personas que se dedican a este tipo de actividades, sabiendo que el ataque puede venir tanto desde fuera como desde dentro de su organización.

El modo de hacer distinciones entre los diferentes usuarios, implica la confección de cuentas de acceso personalizadas y un sistema de validación o autenticación que permite o impide el acceso de los usuarios a los recursos disponibles.

Sobre este tema abundaremos más adelante. Por ahora, basta con aclarar que los nombres de red suelen ser un término alfanumérico, o varios separados por puntos, aunque esto depende del tipo de red.

En el caso de las direcciones ocurre algo parecido. La tecnología de red condiciona el tipo de dirección. Para nuestro estudio, nos centraremos en el sistema de direccionamiento IP, que ya conocemos de Unidades anteriores.

Si el host que pretendemos configurar va a estar en Internet, su dirección IP viene condicionada por la normativa internacional de asignación de direcciones IP.

el nodo va a estar en una red de área local, podemos asignarle una dirección elegida entre un rango que la normativa IP ha reservado para estos casos y que vienen especificadas en el RFC 1918. Estos bloques de direcciones son del 10.0.0.0 al 10.255.255.255, del 172.16.0.0 al 172.31.255.255 y del 192.168.0.0 al

192.168.255.255.

## Asignación de nombres

y direcciones

El primer problema al que hay que hacer frente en el diseño de la estructura lógica de la red consiste en la asignación de nombres y direcciones de red a todos los ordenadores que vayan a convivir con ella. Tanto los nombres como las direcciones han de ser únicos en la red, pues identifican a los equipos.

Todo esto apunta a un nuevo problema que siempre hay que tener en cuenta y que afecta a la seguridad de los sistemas: el intrusismo o hacking.

**Contraseña.** Es la cadena de caracteres que codifica una clave secreta de acceso a la red para cada usuario. La contraseña va ligada al nombre de usuario. Proporciona la llave que protege los datos personales del usuario que la posee<sup>1</sup>.

**Nombre completo del usuario.** Es una cadena de caracteres con el nombre completo del usuario. El nombre de usuario suele ser una abreviatura del nombre completo. En este campo se permite un número mayor de caracteres, incluyendo espacios en blanco, para identificar totalmente al usuario. Algunos examinadores de red muestran este nombre al solicitar una inspección de la red.

**Horario permitido de acceso a la red.** Es un campo que describe las horas y los días en que el usuario tiene acceso a la red. En cualquier otro tiempo el usuario no puede presentarse en la red o es forzado a abandonarla. Por defecto, los sistemas operativos de red permiten el acceso de los usuarios cualquier día a cualquier hora.

**Caducidad.** Describe la fecha en que la cuenta expirará. Es útil para cuentas de usuarios que sólo requieren accesos por periodos de tiempo concretos. Al desactivarse la cuenta, se impide que otros posibles usuarios (intrusos) se apropien indebidamente de ella y, por tanto, protegen y descargan al servidor de accesos indebidos o indeseados.

**Directorio particular.** Es el lugar físico dentro del sistema de ficheros de la red en donde el usuario puede guardar sus datos. Al presentarse en la red, el sistema operativo le posiciona en su directorio particular o le concede acceso al mismo.

**Archivos de inicio de sesión.** Permiten configurar un conjunto de comandos que se ejecutarán automáticamente al inicio de la sesión de red. Están ligados a cada cuenta de usuario, aunque se permite que varios usuarios compartan el archivo de inicio.

**Derechos de acceso**

Una vez que se ha identificado a cada usuario con acceso a la red, se pueden arbitrar sus derechos de acceso. Corresponde al administrador determinar el uso de cada recurso de la red o las operaciones que cada usuario puede realizar en cada estación de trabajo. Ejemplo de estas operaciones son el derecho de acceso a un servidor o a otro equipo a través de la red, forzar el apagado de otro equipo remotamente, reiniciar un equipo, cambiar la hora del sistema, etcétera.

Cada recurso, servicio o utilidad tiene, de este modo, una información asociada que le indica quién puede utilizar- los o ejecutarlos y quién carece de privilegios sobre ellos.

No hay que confundir derechos con permisos:

Un derecho autoriza a un usuario o a un grupo de usuarios a realizar determinadas operaciones sobre un servidor o estación de trabajo.

Un permiso o privilegio es una marca asociada a cada recurso de red: ficheros, directorios, impresoras, etc., que regulan qué usuario tiene acceso y de qué manera.

De esta forma, los derechos se refieren a operaciones propias del sistema operativo, por ejemplo, el derecho a hacer copias de seguridad. Sin embargo, un permiso se refiere al acceso a los distintos objetos de red, por ejemplo, derecho a leer un fichero concreto. Los derechos prevalecen sobre los permisos.

Dependiendo del sistema operativo de red, las marcas asociadas al objeto de red varían, aunque en general podemos encontrar las de lectura, escritura, ejecución, borrado, privilegio de cambio de permisos, etcétera.

En redes en las que hay que hacer coexistir sistemas operativos de red de distintos fabricantes, hay que determinar los permisos para cada uno de ellos. A veces los permisos de un tipo de sistema son trasladables fácilmente a otros sistemas, aunque normalmente no coinciden con exactitud. Por ejemplo, en los sistemas

. Cuentas de grupo

Para facilitar las tareas de administración de red, el uso de los servicios o recursos y organizar coherentemente el acceso a la red, existen en los sistemas operativos de red otras entidades de administración denominadas cuentas de grupo o simplemente grupos.

Una cuenta de grupo es una colección de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo se le asigna automáticamente todas las propiedades, derechos, características, permisos y privilegios de ese grupo. En este sentido, las cuentas de grupo proporcionan una forma sencilla de configurar los servicios de red para un conjunto de usuarios de características similares.

### Perfiles de usuario

En ocasiones interesa que el usuario pueda presentarse en más de una estación de trabajo y que esa conexión sea independiente del lugar, haciendo transparente el trabajo en una u otra estación.

Además, puede interesar al administrador tener la posibilidad de forzar el uso de determinados programas o restringir los cambios en la apariencia del interfaz gráfico a ciertos grupos de usuarios. De este modo, los NOS incorporan utilidades que asocian a cada cuenta de usuario o grupo un perfil concreto.

Los perfiles de usuario pueden estar asociados a una estación de red concreta o bien pueden ser depositados en un servidor de red, de modo que cuando un usuario se presenta, se le asocie el perfil de su propiedad independientemente de la estación por la que acceda a la red: son perfiles móviles.

### Sistemas globales de acceso

El crecimiento de las redes y su organización en grupos de trabajo (subredes, dominios, etc.), así como la integración de NOS de distintos fabricantes, ha llevado a diseñar un sistema de presentación de los usuarios más globalizador.

De este modo, el usuario no tiene que presentarse en múltiples sistemas; basta con que se presente en uno de ellos y la red se encarga de facilitarles el acceso a todos los servicios y sistemas de la red en los que tiene derecho de modo automático.

En algunos NOS, como en Windows, se establecen unas relaciones de confianza entre los distintos grupos de red. En las organizaciones en las que el número de nodos es elevado, conviene ordenar todo el conjunto de la red en grupos o dominios. El sistema de cuentas es propio de cada grupo o dominio.

Con el fin de optimizar la organización de la red, es conveniente establecer un dominio maestro centralizador de todas las cuentas de la organización y crear una

serie de dominios poseedores de recursos sobre los que establecer las relaciones de confianza necesarias para su utilización.

En la configuración del sistema habrá que indicar el modo en que se transmitirán las contraseñas de los usuarios, que son informaciones extraordinariamente sensibles y delicadas.

el Directorio

Activo de Microsoft

El Directorio Activo, como su nombre indica, es un servicio de directorio propietario de Microsoft que consiste en una gran base de datos jerárquica (véase Figura 7.6) que organiza todos los objetos necesarios para administrar un sistema Windows en red: usuarios, equipos, datos, aplicaciones, etcétera.

El DA proporciona toda la información necesaria sobre directivas de seguridad y las cuentas de acceso al sistema de cada usuario o grupos de ellos.

Permite la delegación de la administración, es decir, el administrador puede delegar parte de su trabajo en otras cuentas en las que confía.

Gestiona un sistema de nombres articulado y jerarquizado en múltiples niveles agrupando todas las cuentas en unidades organizativas, que se convertirán en unidades específicas de administración.

Gestión de los servicio

Una vez cubierta la fase de acceso a la red, cada usuario podrá utilizar los servicios a los que tenga derecho de acceso. Sin embargo, una consideración previa del administrador debe ser el modo de disponer los servicios. Una buena elección en el diseño de estos servicios proporcionará un mayor rendimiento de la red.

A continuación estudiaremos los parámetros que hay que tener en cuenta para conseguir mayor eficacia en los servicios de red.

Gestión de los discos

En el caso de servidores interesan interfaces rápidos, por ejemplo, discos SCSI, especialmente las últimas versiones de esta tecnología (Ultra/Wide SCSI). En las estaciones de trabajo basta con interfaces IDE o similares. Otros sistemas de red tienen interfaces propietarios para conectar sus discos. Especial importancia cobra la conexión Fibre Channel para la conexión de discos con unas especificaciones de velocidad extremas.



La tendencia actual de los sistemas de almacenamiento se dirige a hacer transparente a los usuarios el lugar y modo en que residen los datos en el sistema, por ello se puede hablar de una auténtica virtualización del almacenamiento, que no es más que un sistema que permite generar y administrar volúmenes virtuales (lógicamente simulados) a partir de volúmenes físicos en disco

La red de comunicaciones y la red de datos

Es frecuente que el volumen de datos a los que se tenga que acceder por una red sea inmenso. En estas situaciones, mover los datos por la red origina fuertes cuellos de botella que hacen que se tengan que modificar las arquitecturas de red para dar respuesta a estas especificaciones tan exigentes, por encima de tecnologías como Gigabit Ethernet o ATM.

Almacenamiento de conexión directa (Direct Attached Storage, DAS). Cada estación de red tiene sus discos y los sirve a la red a través de su interfaz de red. DAS es la solución de almacenamiento natural de cualquier ordenador.

Configuración del correo electrónico

El correo electrónico es una de las aplicaciones de red más utilizadas en las redes de área local corporativas. Proporciona un medio de comunicación eficaz y libre de errores entre los usuarios de la red y puede dejar constancia escrita de los mensajes intercambiados.

Una aplicación completa de correo electrónico consta de un cliente y un servidor. El servidor gestiona los mensajes de modo que lleguen a sus destinatarios. Para ello, a veces ha de pasar los mensajes a los sistemas de correo de otras redes (relay o retransmisión de mensajes). Por ejemplo, si una corporación tiene dos delegaciones situadas en distintas ciudades y quieren conectar sus sistemas de mensajería electrónica, necesitarán un servidor de correo que se encargue de traspasar los mensajes en una y otra dirección, de modo que todos alcancen su destino. Además, los servidores de correo contienen los buzones de sus usuarios, que almacenan sus mensajes en espera de ser leídos.

La operativa que permite enviar un mensaje de correo electrónico tiene los siguientes pasos:

Se ejecuta la aplicación cliente de correo electrónico, presentándose en el sistema a través de su nombre de usuario y su clave de acceso.

El certificado digital es una credencial que proporciona una Autoridad de Certificación que confirma la identidad del poseedor del certificado, es decir, garantiza que es quien dice ser.

Los parámetros que suelen analizar son muy variados y dependen del tipo de protocolo utilizado y del tipo de red, así como de la topología de la misma.

Algunos analizadores de red tienen mecanismos que generan tráfico controlado para observar la respuesta de la red en situaciones concretas a través de un proceso de simulación de situaciones reales.

### Protocolos para la gestión de redes

El crecimiento experimentado por las redes de área local y, sobre todo, la aparición de sistemas distribuidos, ha generado la aparición de técnicas y protocolos especializados en la gestión de redes.

La idea de partida es conseguir que desde un único puesto de la red (el del administrador) denominado con- sola, se pueda monitorizar toda la red.

Estas tecnologías recogen información de cada uno de los nodos, observando el tráfico en cada uno de los segmentos de la red, avisando en el caso de que se llegue a situaciones que el administrador de la red defina como alarmantes.

En muchos sistemas también se permite la reconfiguración de la red y la simulación de situaciones comprometidas para la red.

Por otra parte, se instalan en la red otros programas denominados entidades de gestión, que recogen e interpretan estas alarmas disparando los mecanismos oportunos para informar al administrador de red o corregir los problemas.

Además, las entidades de gestión interrogan periódica- mente a los agentes de red sobre su estado. De este modo, la entidad de gestión se hace una composición de lugar sobre el estado de la red en cada instante.

Posibles soluciones de mejora para estos problemas podrían ser la asignación de máscaras de red más ajusta- das a las necesidades de la propia red, modificaciones en la topología de red, concentrar los nodos que generan mucho tráfico en segmentos de red rápidos, asegurarse de que se cumplen las especificaciones de los fabricantes en cuanto a longitudes de cables y parámetros eléctricos, etc.

### Casos de estudio para el diseño de redes

Seguidamente, presentamos dos casos en donde se sugiere una posible solución dentro del ámbito de las redes de área local sobre necesidades reales de dos

organizaciones. Obviamente, la solución no es única. Está abierta a muchas otras posibilidades. La solución que aquí se ofrece es orientativa.

## Bibliografía

Administración y gestión de una red área local.