¿Cómo administrar una red de área local?

José Ebert Bonilla*

Resumen

Las buenas redes operan sin que se note, esto solamente es posible a través de una infraestructura de administración de red organizada que permita un intercambio y procesamiento de información en forma eficaz y que los recursos de la red sean utilizados en forma optima con una alta satisfacción de los usuarios. En pocas palabras, tener una calidad de servicio de red (QoS) acorde a las necesidades empresariales. La administración de una red de área local engloba una serie de actividades tales como: la gestión de fallas, configuración, contabilidad, seguridad, inventario, mapeo de red y plantación de la infraestructura. Cada una se debe cuidar con detalle. Hay que tener en cuenta que las redes son sistemas sinérgicos, lo cual implica que el descuido en una de sus áreas impactará directa y sustancialmente el desempeño total de la red. El presente artículo tiene como motivación el presentar una visión teórico-práctica de cómo se puede administrar una red de área local en forma eficiente y eficaz con el fin de obtener del usuario una alta satisfacción.

Palabras clave: administración de redes, calidad de servicio, red de área local, análisis de tráfico, seguridad en redes.

How to manage a local area network

Abstract

The best networks work so efficiently that we do not notice them. It is only possible through an infrastructure of management of organized network, which allows an efficient information interchange and processing, the network resources are used are optimally with a high satisfaction by users. In few words, it means to have a quality of service appropriate to entrepreneurial needs. The management of a local area network comprises a series of activities such as failure management, configuration, accounting, security, inventory, network mapping and infrastructure. Each one must take care of the details. We have to take into account that networks are synergic systems; it implies that a failure in any of the areas will have direct effects on the performance of the whole network. This article intends to present a theoretical and practical view of how to manage a local area network efficiently and effectively in order to have a high satisfaction by users.

Key words: network management, quality of service, local area network, traffic analysis, security in networks.

* Ingeniero de Sistemas Universidad Católica de Colombia. Especialista en Gerencia de Tecnología de la EAN. Actualmente desarrolla Maestría en Ciencia de la Información y Telecomunicaciones en la Universidad Distrital de Bogotá. Profesor de la Facultad de Ingeniería de Diseño y Automatización Electrónica. Correo electrónico: ebert@etb.net.co

Fecha de recepción: octubre 10 de 2005.
Fecha de aprobación: octubre 14 de 2005.

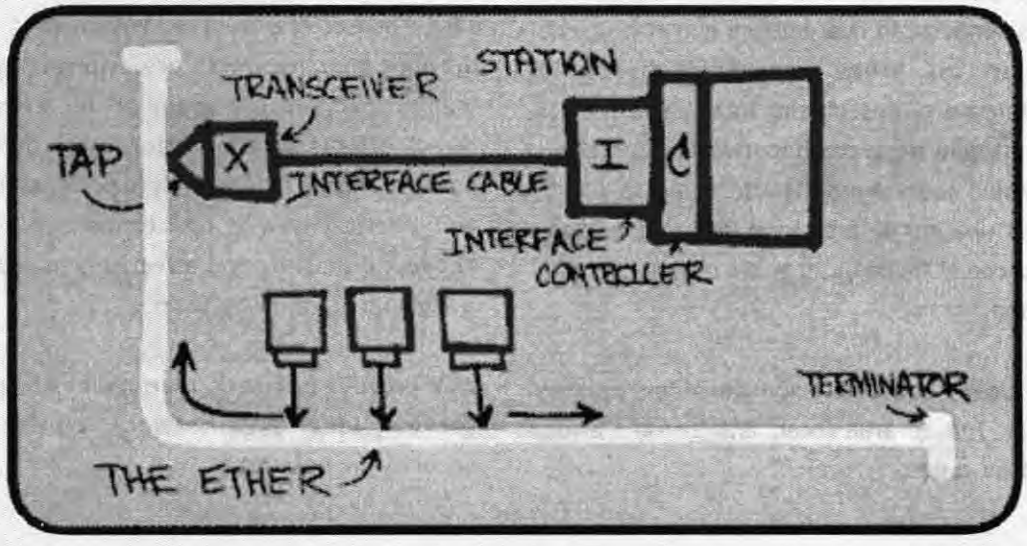
En los años 70, Robert Metcalfe y David Bogas, trabajaban para Xerox en ese entonces, inventaron una forma en la cual se podían comunicar computadores que se encontraban a distancias no mayores de 2800 mts[1], y a una velocidad de 10 Mega bits por segundo[2].

En los años 80, se entrega al mercado de consumo un elemento tecnológico que revolucionó el mundo, el Personal Computer (PC). La revolución consistió en poner la computación al servicio y en manos de las personas del común.

Los dos hechos anteriormente descritos, inevitablemente tuvieron una convergencia[3]. El auge de la computación llevo a que en pequeñas áreas (el espacio de una oficina, el piso de un edificio o un edificio) se tuviera una densidad de computadores personales bastante apreciable. Unido a lo anterior, se tenía una nueva arquitectura de red que permitía el flujo de información a «alta velocidad». A este tipo de redes se les denominó redes de área local.

Las aplicaciones de *software* empresarial ejecutadas en los PC tuvieron un aumento exponencial y al lado de ellos, la interconexión de los mismos. Pero este crecimiento casi desbordado trajo consigo la presencia de fallas difíciles de detectar, congestión de tráfico en los canales de comunicación, pérdida de la noción de la topología de la red, disminución de la seguridad en el transporte y almacenamiento de la información y pérdida de la confidencialidad y veracidad de la misma. La generación de malestar e insatisfacción dentro de los usuarios no se hizo esperar. Por estas razones, la calidad del servicio decayó ostensiblemente, a tal punto que dio la idea de que la red ya no cumplía con los servicios para los cuales fue creada.

Gráfica 1. Plano en borrador de la red Ethernet



1 A esta red se le denominado Ethernet. La Gráfica 1 presenta el plano en borrador de dicha red. Esta gráfica fue tomada de la página Web de Xerox.

2 Es de anotar que esta velocidad era muy alta en ese tiempo. La velocidad que se lograba por pares aislados no era mayor a 9600 bits por segundo. Esta velocidad se obtenía cuando las condiciones de comunicación y los enlaces estaban en óptimas condiciones.

3 Esta convergencia es propiciada por el uso cada vez más común de elementos de procesamiento en las comunicaciones, lo cual las hacía más eficientes: debido al proceso de digitalización de todo tipo de información y a la necesidad de compartir información en forma fácil y en tiempo real.

Siguiendo el proceso evolutivo, las tecnologías de las redes tuvieron un momento de caos, en el cual, tanto los productores de *software* como de *hardware* para redes, se dieron cuenta que era necesario poner en práctica buenas prácticas tecnológicas, de uso y administración de las redes de comunicación de datos; de tal forma que se lograra el crecimiento de las mismas, en forma ordenada y manteniendo una calidad de servicio satisfactoria para los usuarios finales.

El proceso inició por una serie de recomendaciones a través de lo que se denominan los *DRAFT*, algunas de estas recomendaciones se convirtieron en protocolo, otras en *software* y algunas otras en metodologías y procedimientos. Con el pasar del tiempo y con los desarrollos tecnológicos, los proveedores de tecnología decidieron recoger todo esto en una sola solución integrada de gran envergadura.

Cabe anotar que la administración de redes no solo se trata de elementos técnicos y tecnológicos que nos permitirán hacer un manejo adecuado de la red; sino también se debe tener en cuenta que a lo anterior hay que sumarle un personal debidamente entrenado y una administración altamente prospectiva y proactiva, con lo cual, podrá tomar decisiones acertadas oportunas y eficientes.

Cuando se debe pensar en administrar una red

Se puede suponer que una red con dos usuarios no necesitará un despliegue técnico y humano para administrarla, en esos casos, se le asigna la administración a cada uno de los usuarios quienes serian directamente los responsables.

El manejo de las redes comienza a ser vital cuando tenemos que manejar alguna o todas las variables, que a continuación se nombran:

- Redes físicamente dispersas.
- Incremento del uso de la red (aumento de tráfico).
- Necesidad de discriminación entre usuarios.
- Interconexión con otras redes (conexión a internet, redes WAN, generación de extranets, etc.).
- Un número superior a 15 usuarios.
- Implementación de redes privadas virtuales.
- Tiempos de respuesta muy largos.
- Necesidad de administración de seguridad.

Si se observa que algunos o todos los enunciados anteriores se están presentando en una red, es hora de iniciar la generación de políticas de administración de red y por que no de un sistema de administración de redes locales[4] y de la búsqueda una persona idónea para que se haga cargo de la administración de la red. Claro esta, que si se ha hecho un análisis y diseño detallado de la red, estos puntos estarán cubiertos antes que se sucedan.

Una de las metas de la administración de redes es lograr anticiparse a los problemas, esto permitirá que se ejerza una labor silenciosa pero eficiente, obteniendo una calidad del servicio superior a las necesidades de la empresa.

4 El uso de un sistema de administración de redes va a depender del tamaño de la red y de los recursos con que cuente la empresa para tal fin.

Principales funciones de la administración de redes

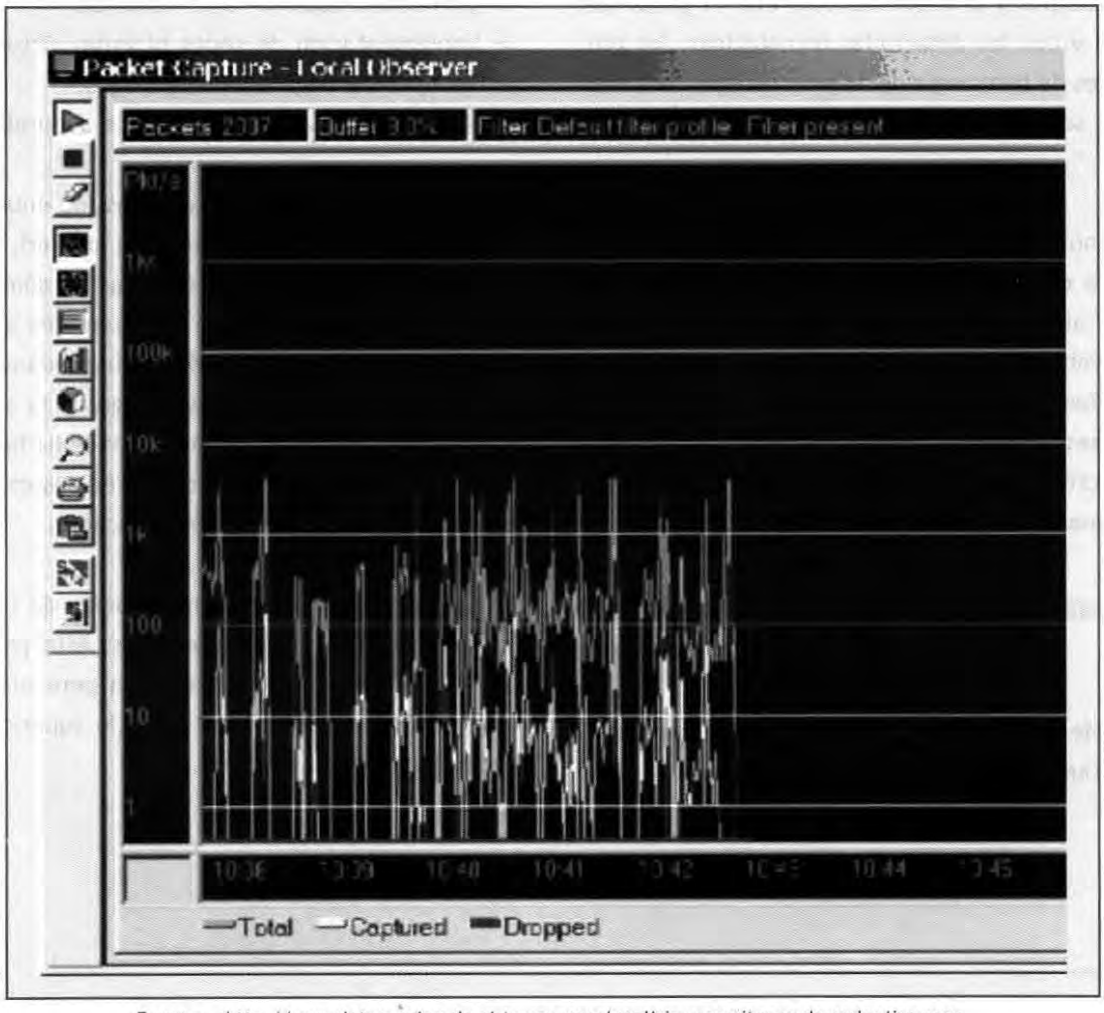
Existen ocho tareas básicas que se deben desarrollar cuando se está administrando una red de área local. Dependiendo de la magnitud de la red y del uso que se le este dando se tendrán en cuenta todas o parte de ellas. Lo que sí es necesario saber, es que el orden en el cual aparecen es el orden de importancia que cada una tiene.

- Análisis de rendimiento.
- Seguridad.
- Monitoreo de fallas.
- Control de configuración.
- Mapa de la red.
- Manejo de inventario.
- Planeación de red.
- Contabilidad de costos.

En los párrafos siguientes, se presenta una revisión de cada uno de los aspectos relacionados en la lista anterior.

Análisis de rendimiento

Este análisis involucra: el monitoreo de la cantidad de tráfico en la red, el uso de los recursos y el mantenimiento del archivo histórico (*logs* de auditoria).



Fuente: <http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/images>

Esta labor está encaminada a mantener en nivel adecuado la velocidad de prestación de servicios y el tiempo promedio de respuesta que experimenta cada uno de los usuarios de la red.

A través de una serie de mediciones de tráfico[5], se pueden obtener cantidad de datos que permiten establecer parámetros estadísticos[6], por medio de los cuales se determina el comportamiento de la red.

La medición de tráfico se debe realizar en diferentes días, a diferentes horas. Es de suma importancia saber las horas y días de máximo y mínimo tráfico; que son los momentos más propicios para desarrollar esta actividad. De igual relevancia es el determinar las áreas y los equipos que generan el mayor flujo de información.

En el momento de realizar el análisis de los datos obtenidos en las diferentes mediciones, se debe tener en cuenta que tipo de protocolo o pila de protocolos se está usando en la red. Este ítem, permite determinar si el *overhead* es alto o bajo, porque cada protocolo maneja diferentes tamaños de encabezados, lo cual marca una diferencia en el contenido de información en los datos recogidos.

Dentro del análisis de rendimiento, es necesario hacer una revisión de los enlaces virtuales que se establecen entre los diferentes usuarios de la red. La razón para realizar esta revisión está sustentada en el hecho de los usuarios establecen estos enlaces virtuales, los cuales son usados esporádicamente, pero saturando los recursos y causando una sobrecarga en la red.

Los sistemas operativos actuales incluyen algunas herramientas que permiten hacer un monitoreo de red básico; con sistemas de administración de red actuales, se puede hacer un monitoreo completo y en tiempo real, mostrando los resultados a través de gráficas explicativas y que permiten que el administrador tome decisiones en forma oportuna.

Las soluciones que se pueden implementar para obtener un mejor desempeño en la red pueden ser la implementación de soluciones de baja o alta complejidad, económicas o costosas; todo depende de la infraestructura tecnológica con que se cuente y con el presupuesto asignado para tal fin. Algunas de las opciones a las que se puede acceder para mejorar el rendimiento son:

- Incremento en la potencia y capacidad de almacenamiento de los servidores.
- Incremento en el número de servidores.
- Cambio de tarjetas de red para el aumento de la velocidad.
- Segmentación de red.
- Cambio en el patrón de uso de la red.
- Cambio de tipo de red.
- Cambio de cableado.
- Cambio de *backbone*.
- Mejora o cambio de lo elementos de interconexión activos (*router*, *switch*, etc.).

Lo anterior se aplica de acuerdo a los resultados arrojados por las estadísticas.

Se puede encontrar el caso de un cuello de botella en un servidor de uso múltiple (comunicaciones, aplicaciones, impresión, etc.); en este caso, la solu-

5 Se sugiere que las mediciones de tráfico se efectúen en diferentes puntos de la red, a diferentes horas del día y teniendo en cuenta los días de más alto volumen de tráfico, si estos llegaran a existir.

6 Algunos de los parámetros estadísticos a tener en cuenta pueden ser promedio de paquetes enviados, recibidos, retransmisiones, overhead, tráfico efectivo tasa de errores, entre otros.

ción más conveniente es distribuir las tareas en otros servidores que se tengan en la red y que posean capacidad para ejecutar la tarea. En caso de no poder implementar esta solución, debido a la baja capacidad de los servidores, se hace necesario aumentar el número de servidores.

Pero igualmente se puede detectar que el problema es la lentitud del servidor, entonces se deben buscar posibles alternativas, tales como hacer una actualización del procesador, aumentar la memoria o la utilización de memoria *cache*. Si el problema es espacio de almacenamiento secundario, un aumento de disco estaría bien o se puede llegar a ser más radical, dependiendo de la gravedad del problema y llegar al cambio del servidor por uno nuevo con una configuración de mayor potencia a la actual. En este último caso, es de vital importancia contemplar el crecimiento que presentará la red en el mediano plazo, esto con el fin de no tener un servidor obsoleto muy pronto.

Pero no solo los servidores son los culpables de la degradación del rendimiento de la red, otro cuello de botella se puede presentar en los elementos activos (*router, switch, gateway,* etc.); para estos casos, es necesario pensar en un cambio del dispositivo de mayor velocidad o efectuar otro tipo de segmentación de tráfico.

Otro elemento que puede afectar el rendimiento de la red es el cableado o el *backbone*. Para este caso, se puede pensar en el cambio de tipo de cableado y si es el caso, se puede pensar en fibra óptica.

Seguridad

El tema de la seguridad cada día tiene más preponderancia en el ámbito de la administración de redes de transmisión de información. El uso intensivo de la red de redes: internet por parte de las empresas y de la comunidad en general, la vinculación de las redes corporativas a esta y la existencia de usuarios de todo tipo y de muy variadas intenciones han magnificado el tema, hasta el punto de crear una paranoia en cuanto a seguridad de la información se refiere. La seguridad está encaminada a proteger los datos y los equipos de daños accidentales o mal intencionados.

Los actuales sistemas operativos de red han implementado una protección para el acceso tanto a nivel local como a nivel de red (recursos compartidos) con el fin de evitar acceso a la red por personas no autorizadas. Pero esto no es suficiente. Se requiere la incorporación de nuevo *hardware* y *software* que haga frente a los diferentes peligros a los cuales está expuesta la información.

Si bien es cierto, los sistemas operativos han traen implementados unos mecanismos de validación de acceso, estos no son suficientes. Se requiere contar con elementos tales como *routers* de selección, *firewalls, proxys,* NAT, mecanismos de encriptación de llave pública o llave privada, etc. Algunos de ellos son netamente *hardware*; otros están implementados en *software*; pero la mayoría es una combinación; buscando mayor rapidez sin hacer un amplio sacrificio de la flexibilidad. Cabe anotar que la implementación de estrategias de seguridad conlleva un costo asociado, el cual puede ser alto. Para determinar si es necesario hacer la inversión, lo primero que se tiene que hacer es estimar el valor de la información que se quiere proteger y luego compararlo con el costo del sistema de seguridad. Una de las medidas que en cualquiera de los casos se debe implementar y que no tiene un costo directo es la activación de los *logs* de auditoria; a través de ellos, se pueden establecer las acciones ejecutadas por los usuarios de la red o por intrusos.

Otro tipo de seguridad que se debe implementar es la defensa contra los «patógenos»: virus electrónicos y esto se puede lograr haciendo uso de *software* legal, sin descargar *software* de internet de dudosa procedencia y ante todo, contar con un antivirus que nos asegure, en alguna medida, la no entrada de virus al sistema. Una de las formas más fáciles de contaminar los equipos existentes en una empresa es a través de la red; una recomendación es no usar dos o más antivirus al tiempo, esto no genera mayor protección; por el contrario, hace su infraestructura más vulnerable.

Se ha hablado de la protección lógica que se le debe dar a los datos, pero igualmente importante, es darle protección física a los servidores y demás elementos que conforman la red. Es aconsejable tener los servidores en lugares de área restringida; ya que en algunos casos, son equipos que tienen información crítica para la empresa y en el momento de producirse un accidente, pueden causar pérdidas incalculables. En cuanto a los otros elementos de la red, es aconsejable que estos se encuentren ubicados en gabinetes con su respectiva protección.

En cuanto al cableado, no sobra decir que es imprescindible que el tendido se encuentre dentro de su respectiva canaleta metálica o en una coraza metálica. No es para nada aconsejable el uso de canaletas plásticas. La razón por la cual se debe usar canaleta metálica es por que con ella se consigue formar la denominada cámara de Faraday, lo cual aísla el cableado de inducciones magnéticas externas que puedan generar errores en la transmisión de los datos.

Monitoreo de fallas

Una buena fórmula para contrarrestar las fallas, es tener copias de seguridad de la información. Por normas de auditoria es necesario tener tres copias distribuidas en distintos lugares a fin de poder responder con prontitud frente a cualquier contingencia.

Es recomendable que las fallas presentadas se documenten con el ánimo de llevar una bitácora adecuada que permita a otro saber como actuar frente a estas fallas. Igualmente, es aconsejable que se haga un seguimiento minucioso con el fin de poder determinar las causas y poner en marcha planes que aseguren que estas fallas no se repitan.

Acciones para aprovechamiento

Existen algunas acciones que podemos tomar a fin de poder asegurar un alto porcentaje de disponibilidad de la red, estas son:

- Detectar alguna falla que haya sucedido o esté por suceder.
- Minimizar el impacto de las fallas.
- Adecuado soporte para el arreglo de problemas.

Cuando se cuenta con un buen sistema de administración de redes es posible que se hagan previsiones sobre una posible falla en la red o en los equipos que se encuentran conectados a ella. Igualmente podemos tener facilidad de hacer *bypass* a los equipos que se encuentren fallando con el ánimo de evitar que degraden la red.

Otro aspecto que se debe tener en cuenta, es la minimización del impacto que ocasionan las fallas en los usuarios. Se debe tener procedimientos de contingencia que permitan, si es posible, que los usuarios no se den cuenta de las fallas que suceden en la red.

Por otra parte, el administrador de la red debe contar con terceras partes que le proporcionen mantenimiento a los equipos y a la red en tiempo récord

(es deseable que se en termino de horas). Para lograr esto, es necesario establecer alianzas estratégicas con el proveedor de mantenimiento, así se hará más fácil lograr este tipo de prioridades.

Disponibilidad de los servidores

Una de las medidas que podemos tener en cuenta para proveer disponibilidad de la red es tener siempre en funcionamiento los servidores y esto se obtendrá a través de los sistemas operativos de red local o del *software* de red o por medio de utilitarios.

Los sistemas operativos actuales proporcionan utilitarios tales como el escáner de disco al iniciar la sesión, con el fin de proporcionar un medio seguro de almacenamiento al usuario.

Si nuestro sistema operativo no tiene estas posibilidades, debemos implementar las siguientes recomendaciones:

- Que se haga una verificación de lectura después de escribir.
- Seguimiento de las transacciones.
- Discos espejados y duplicidad de disco.
- Servidores espejados.
- Fuentes de poder ininterrumpibles (UPS).

Control de configuración

Para el manejo de la configuración de la red se lleva a cabo de forma automática, de esta manera se facilita tanto la actualización de la información, como su consulta; además que podemos disponer de un gran número de copias en poco tiempo y a bajo costo.

Los ítems de los cuales es necesario tener la configuración son los siguientes:

- Cableado.
- Equipos de computo.
- Servidores.
- Estaciones de trabajo.
- Equipos de comunicación.
- HUB.
- *Router*.
- *Switch*.
- *Bridges*.
- *Gateway*.
- *Firewalls*.
- Otros.

En caso que los equipos estén conformados tanto de parte física como lógica, se hace necesario llevar registro de ambas partes.

La actualización de la configuración de antemano nos está garantizando tener un inventario de todos los elementos que conforman la red. Además que nos ayudará a que los cambios o modificaciones que se efectúen, estén sustentadas sobre el estudio previo de las configuraciones existentes, lo que proporcionará alta probabilidad de no ocasionar traumatismos.

Planeación de la red

La planeación de red se refiere a las reformas que se vislumbran venir, tales como el crecimiento de usuarios en la red, actualización de *software*, comunicación con otras redes o sistemas y todo aquello que de una u otra forma, afecte a los usuarios.

Este tipo de trabajos se deben prever con anterioridad y se deben estipular los días en los cuales se realizaran; en lo posible, se deben efectuar los días en los cuales no hay usuarios conectados a la red (domingos o feriados), a fin de no entorpecer el trabajo de ellos y así el administrador puede hacer

todas las pruebas pertinentes a fin de certificar que todo está trabajando satisfactoriamente.

Esta planeación no solo debe responder a las necesidades que se van presentando como evolución natural de la red sino también a una constante actualización del administrador que le permita incorporar nuevos productos y nuevos equipos a la red, a fin de mejorar los servicios presentes o implementar unos nuevos que aumenten el bienestar y la productividad de los usuarios.

Contabilidad de costos

Esto es propio de empresas que cuentan con redes grandes y que se encuentran divididas en departamentos y donde a cada departamento se le carga el costo de tener la red en funcionamiento.

Para nadie es un secreto que el poner en funcionamiento una red conlleva una serie de costos (que al inicio son altos), los cuales hay que ponerlos en confrontación con los beneficios obtenidos y se busca que la relación establecida entre estas dos cantidades sea mayor a uno (1). Es bueno decir que en una red se tendrán costos cargables a lo largo del periodo de vigencia o utilización de la red.

Mapa de la red

Este mapa de la red debe ser otra de las utilidades que proporcione al sistema el administrador de la red y debe ser lo suficientemente potente y amigable para que permita el manejo de la configuración y también que a través de él, se logre visualizar el punto donde se ha detectado una falla.

Se pueden tener dos tipos de mapas: geográfico y topológico. El mapa geográfico es necesario cuando tenemos un gran número de redes LAN dispersas en diferentes localidades, las cuales tenemos interconectadas. Este tipo de mapa mostrará la ubicación geográfica de cada uno de los elementos que componen la red.

El mapa topológico servirá para visualizar los dispositivos y enlaces establecidos entre ellos sin interesar si ellos se encuentran en su posición geográfica exacta. Este es muy usado para redes pequeñas.

Dependiendo de la magnitud de la red y de su distribución se puede usar uno o el otro, o en algunos casos es aconsejable el uso de ambos o un híbrido para lograr tener una mayor claridad de la magnitud de la red y sus implicaciones.

Manejo de inventarios

Este concepto está directamente ligado con el mapa de la red y con el manejo de la configuración. Esta administración se debe hacer independientemente de si la red es pequeña o grande.

La utilización se puede ver desde varios ángulos y uno de ellos es llevar el registro de los equipos que se han utilizado a lo largo del ciclo de vida de la red, lo que dará casi que un historial de la evolución. También se puede utilizar en casos de tener alguna falla lógica o física en la red reportada por un usuario; rápidamente podemos ver, a través del inventario, cual es la configuración de ese punto y determinar si la falla es generada ahí o en otro punto.

Conclusiones

Podemos concluir afirmando que la administración de redes es la colaboración cooperativa tanto de la parte humana, como de la parte técnica y además debe ser una convicción de la alta gerencia, tener la visión necesaria para entender hay que disponer recursos suficientes para este tipo de labor.

También se debe tener consciencia de que la implementación de administración de redes implica asumir costos, los cuales en muchas ocasiones la alta gerencia no está dispuesta a sufragar, pero es trabajo de la persona que tiene a cargo la administración de la red convencer a la gerencia que en caso de no invertir en este rubro, la empresa estará trazando un camino hacia el caos en lo que se refiere a su parte de tecnologia en informática y más exactamente en su parte de redes.

Por ningún motivo se debe descuidar lo concerniente a la seguridad. Esta es una de las tareas que ha tomado mayor importancia al interior de las organizaciones. Las pérdidas por este concepto son muy altas y tienen implicaciones no solo a nivel económico, sino legal, competitivo y de imagen corporativa.

Bibliografía

Ahuja, V. *Design and análisis of computer communications networks.* Singapore: McGraw Hill, 1982.

Derfler, F. *Descubre Redes Lan & Wan, Claro. Conciso. Confiable.* Madrid: Prentice Hall, 1998.

Hunter, P. *Local Area Network, Making the right choice.* Great Britain; Addisson Wesley, 1993.

McClure, S. *Hackers. Secretos y Soluciones para la seguridad de redes.* España: McGraw Hill, 2000.

Northcutt, S. *Detección de Intrusos. Guia Avanzada. 2da. Edición.* España: Pearson Educación, 2001.

Piattini, M. *Auditoria Informática. Enfoque práctico.* Alfaomega, 1998.