

PRINCIPIOS FUNDAMENTALES PARA EL DESARROLLO Y ADMINISTRACIÓN EFICIENTE DE REDES DE COMPUTADORES LAN EN LA FÁBRICA

José Ebert Bonilla
Candidato a Magíster
Corporación Universitaria Unitec

Jaime Humberto Carvajal, M. Sc.
Universidad de La Salle

Resumen

Las buenas redes operan sin ser percibidas, y esto sólo es posible con una infraestructura de administración de red organizada que permita, a la vez, el intercambio y procesamiento de información en forma eficaz y una óptima utilización de los recursos de la red con una alta satisfacción de los usuarios. 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 de las cuales se debe atender en detalle. Hay que considerar que las redes son sistemas sinérgicos, lo cual implica que el descuido en una de sus áreas impactará directa y sustancialmente en el desempeño total de las mismas. El presente artículo presenta una visión teórico-práctica de los principios fundamentales para administración eficiente de redes de computadores LAN.

José Ebert Bonilla es ingeniero de sistemas de la Universidad Católica de Colombia, especialista en Gerencia de Tecnología (EAN) y candidato a Magíster en Ciencia de la Información y Telecomunicaciones de la Universidad Distrital de Bogotá. Es el actual jefe de los programas de Tecnología en Sistemas, y Electrónica y Telecomunicaciones, Corporación Universitaria Unitec; jbonilla@unitec.edu.co. Jaime Humberto Carvajal Rojas es ingeniero mecánico de la UFPS (Cúcuta, Colombia), magíster en Sistemas Automáticos de Producción (UTP) y doctor en Ingeniería Mecánica con especialización en Ingeniería Mecatrónica y Robótica Industrial (Universidad Estatal de Campinas UNICAMP, Brasil). Decano Facultad de Ingeniería de Diseño y Automatización Electrónica de la Universidad de La Salle; jcarvajal@lasalle.edu.co.



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

Introducción

En los años 70, Robert Metcalfe y David Bogas (ver Ahuja, 1982), quienes en ese entonces trabajaban para Xerox, inventaron un sistema mediante el cual se podían comunicar computadores que se encontraran a distancias no mayores de 2.800 m,¹ a una velocidad de 10 Megabits por segundo.²

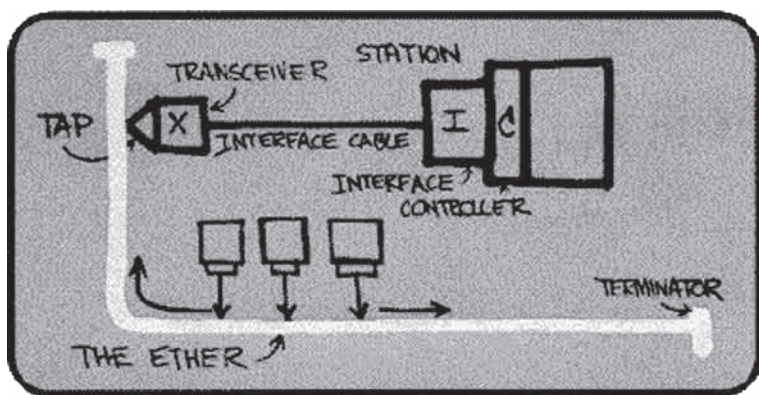


Figura 1. Plano en borrador de la red Ethernet.³

En los 80, se entrega al mercado de consumo un elemento tecnológico que revolucionó el mundo, el PC (Personal Computer). La revolución consistió en poner la computación

al servicio y en manos de las personas del común (Derfler, 1998).

Los dos hechos inevitablemente tuvieron una convergencia.⁴ El auge de la computación llevó 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 no fáciles 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 sensación de malestar e insatisfacción dentro de los usuarios no se hizo esperar. Resumiendo, 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 había sido creada.

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 consideraron necesario aplicar prácticas tecnológicas de



uso y administración de las redes de comunicación de datos, de tal forma que se logrará 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 los denominados DRAFT. Algunas de dichas recomendaciones se convirtieron en protocolo, otras en software y algunas más en metodologías y procedimientos. Con los desarrollos tecnológicos, los proveedores decidieron recoger todo esto en una única solución integrada de gran envergadura.

Cabe anotar que la administración de redes no tiene que ver únicamente con elementos técnicos y tecnológicos que permitan hacer un manejo adecuado de la red, sino que también hay que sumarle un personal debidamente entrenado y una administración altamente prospectiva y preactiva, con lo cual se podrán tomar decisiones acertadas, oportunas y eficientes.

Administración de una red

Una red con dos usuarios no necesita un despliegue técnico y humano para administrarla. En estos casos se le asigna la administración a cada uno de los usuarios, quienes son directamente responsables. Pero la administración de una red con muchos usuarios se vuelve compleja, ya que intervienen muchas variables:

- 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.
- Tiempo de respuesta muy largos.
- Necesidad de administración de seguridad.

Una de las metas de la administración de redes es anticiparse a los problemas, lo que permite ejercer una labor silenciosa pero eficiente, obteniendo una calidad de servicio superior a las necesidades de la empresa. En este caso es necesario generar políticas de administración de red o un sistema de administración de redes locales,⁵ además de seleccionar una persona idónea para la administración de la misma.

Principios de administración de redes

Existen ocho principios básicos para la administración de

una red de área local, dependiendo de la magnitud de la red y de su aplicación, pero es necesario el orden de los mismos:

1. Análisis de rendimiento.
2. Seguridad.
3. Monitoreo de fallas.
4. Control de configuración.
5. Mapa de la red.
6. Manejo de inventario.
7. Planeación de red.
8. Contabilidad de costos.

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 auditoría).

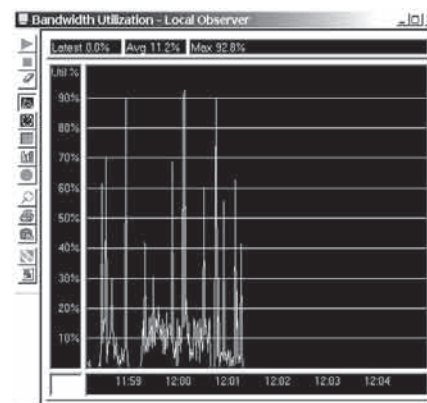


Figura 2. Detalle del análisis de rendimiento de una LAN.⁶

Esta función está encaminada a mantener un nivel adecuado en 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 tráfico⁷ se puede obtener una gran cantidad de datos que permiten establecer parámetros estadísticos,⁸ por medio de los cuales se determina el comportamiento de la red.

La medición de tráfico se debe realizar en diferentes días y a diferentes horas. Es de suma importancia conocer las horas y días de máximo y mínimo tráfico, que son los momentos más propicios para desarrollar esta actividad. Igual relevancia tiene 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 considerar el tipo de protocolo o pila de protocolos que se están 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 de los datos recogidos.

Dentro del análisis de rendimiento es necesario revisar los enlaces virtuales que se establecen entre los diferentes usuarios de la red. Dicha revisión se apoya en el hecho de que los usuarios establecen estos enlaces virtuales, que son usados esporádicamente pero saturan los recursos y causan una sobrecarga en la red.

Los sistemas operativos actuales traen incluidas 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 muy dicentes que permiten que el administrador tome decisiones en forma oportuna.

Para obtener un mejor desempeño en la red se puede pensar en una implementación de soluciones de baja o alta complejidad, baratas o costosas dependiendo 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 los elementos de interconexión activos (router, switch, etc.).

Todo lo anterior se aplica de acuerdo con 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.), caso en el cual la solución más conveniente es distribuir las tareas en otros servidores que se tengan en la red y que posean la capacidad para ejecutar la tarea. En caso de no poder implementar esta solución, por 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 debe pensar en

posibles alternativas tales como hacer una actualización del procesador, un aumento de memoria o la utilización de memoria caché. Si el problema es de espacio de almacenamiento secundario, un aumento de disco estaría bien, aunque se puede ser más radical dependiendo de la gravedad del problema, llegando al cambio del servidor por uno nuevo con una configuración de mayor potencia al actual. En este caso, es de vital importancia el 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 sólo los servidores son los culpables de la degradación del rendimiento de la red, ya que otro cuello de botella se puede presentar en los elementos activos (router, switch, gateway, etc.). En este caso es necesario pensar en un cambio del dispositivo de mayor velocidad o efectuar otro tipo de segmentación de tráfico.

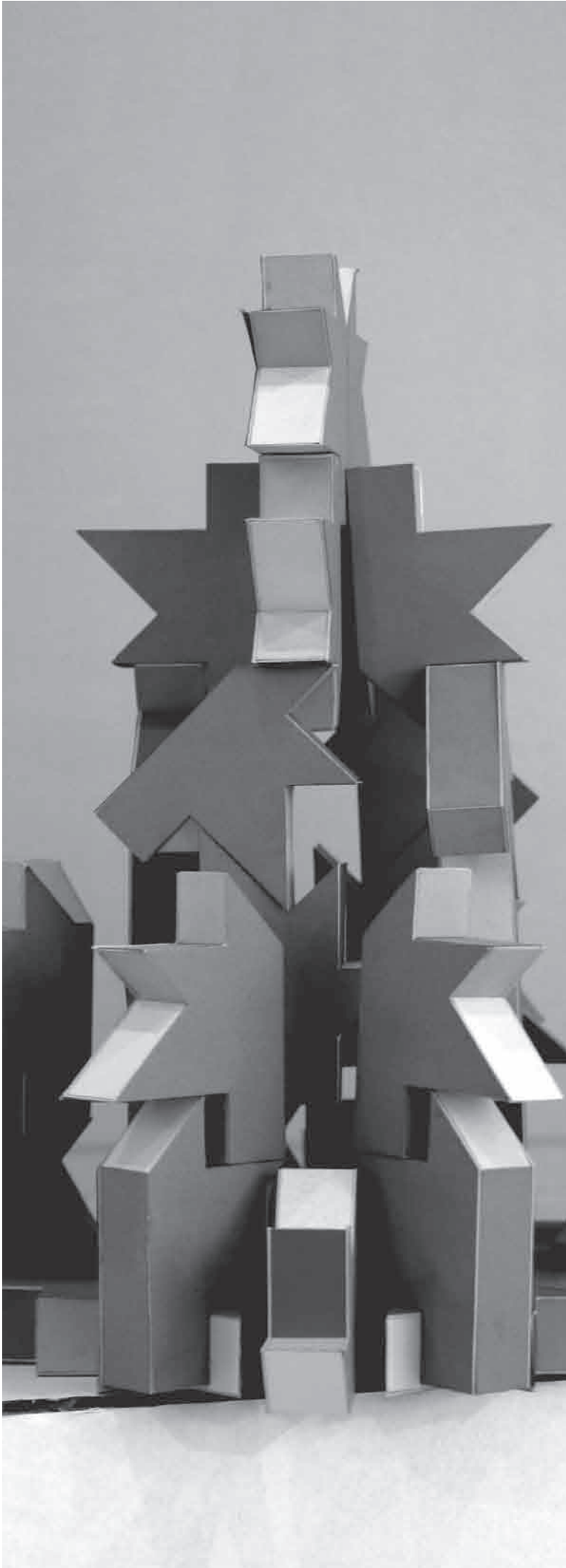
Otro elemento que puede afectar el rendimiento de la red es el cableado o el backbone, caso en el cual se puede optar por el cambio de tipo de cableado o, si es el caso, pensar en fibra óptica.

Seguridad

La seguridad tiene cada día 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 ésta 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 se 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 el acceso a la red por parte de personas no autorizadas. Pero esto no basta, ya que se requiere la incorporación de nuevo hardware y software que haga frente a los diferentes peligros a los cuales está expuesta la información.

Usualmente los sistemas operativos traen implementados unos mecanismos de validación de acceso, los cuales no son suficientes. Para la seguridad en la red LAN se requieren elementos como routers de selección, firewalls, proxys, NAT, mecanismos de encriptación de llave pública o llave privada, etc. Algunos de estos son



hardware, mientras que otros están implementados en software, pero en la mayoría de los casos se trata de una combinación, buscando con esto mayor rapidez sin hacer un amplio sacrificio de la flexibilidad. Cabe decir que la implementación de estrategias de seguridad conlleva un costo asociado que 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 log de auditoría, porque a través de ellos se pueden llegar a establecer las acciones ejecutadas por los usuarios de la red o por intrusos.

Otro tipo de seguridad que debe implementarse es la defensa contra los "patógenos" virus electrónicos, y esto se puede lograr haciendo uso de software legal, no bajando software de Internet de dudosa procedencia y, ante todo, teniendo 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 le da mayor protección, por el contrario, hace su infraestructura más vulnerable.

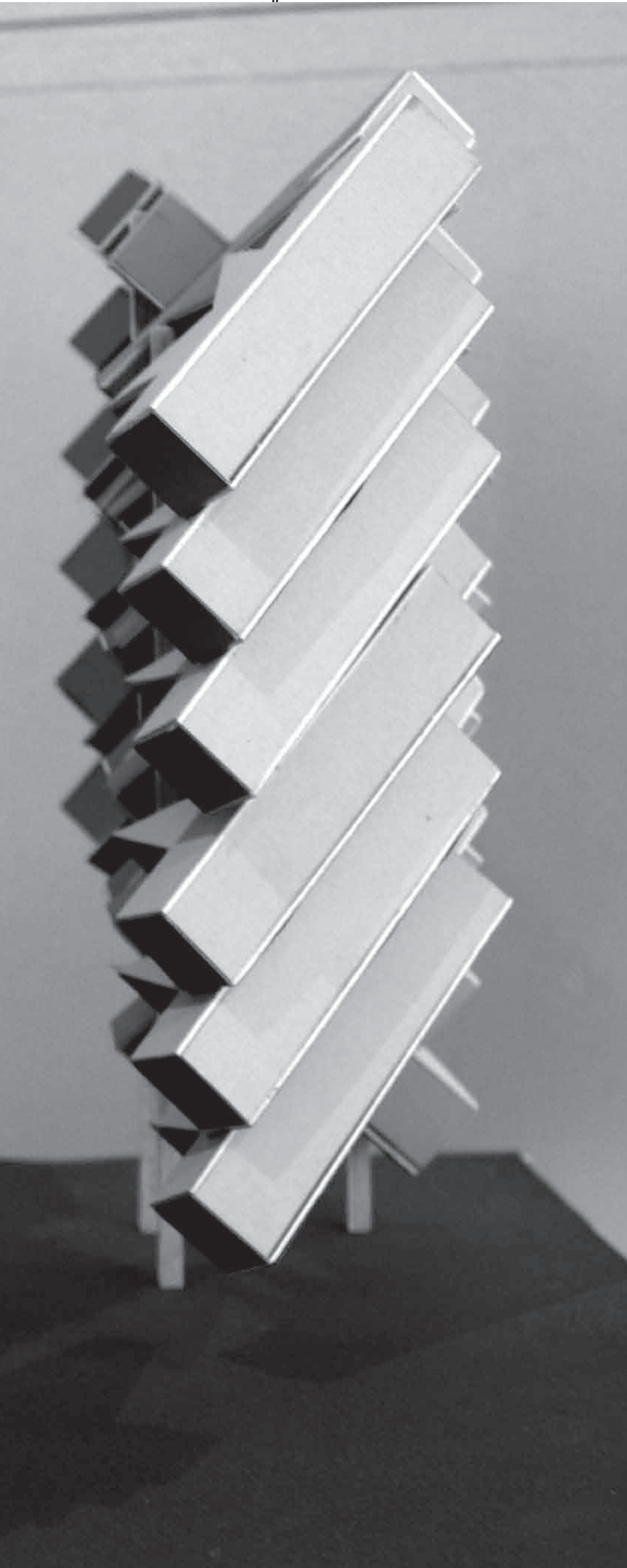
Se ha hablado de la protección lógica que se le debe brindar a los datos, pero también es importante darle protección física a los servidores y demás elementos que conforman la red. Es aconsejable mantener los servidores en lugares de área restringida, ya que en algunos casos son equipos que tienen información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

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

Monitoreo de fallas



Una forma para contrarrestar las fallas es poseer copias



de seguridad de la información. Por normas de auditoría 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 otra persona saber cómo actuar frente a dichas 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.

Existen acciones a tomar con el fin de poder asegurar un alto porcentaje de disponibilidad de la red:

- 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 provisiones sobre una posible falla en la red o en los equipos que se encuentran conectados a ella. Igualmente, se debe tener facilidad de hacer *bypass* a los equipos que se encuentren fallando, evitando así que degraden la totalidad de la red. Otro aspecto a considerar es la minimización del impacto que ocasionan las fallas en los usuarios. Se deben tener procedimientos de contingencia que permitan, en lo posible, que los usuarios no se enteren de la falla en la red.

El administrador de la red, por otra parte, debe apoyarse en personal de mantenimiento a los equipos y a la red en tiempo récord, deseable en término de horas, además de establecer alianzas estratégicas con el proveedor.

Una de las medidas a tomar para proveer disponibilidad de la red es tener siempre en funcionamiento los servidores, lo cual 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 escaneo de disco al iniciar la sesión, con el fin de proporcionar un medio seguro de almacenamiento al usuario. Si el sistema operativo no tiene estas posibilidades, entonces se debe, en lo posible, tratar de 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

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

Los principios a considerar para el control de configuración, entre otros, son los siguientes:

- Cableado.
- Equipos de cómputo.
- Servidores.
- Estaciones de trabajo.
- Equipos de comunicación.
- HUB.
- Router.
- Switch.
- Bridges.
- Gateway.
- Firewalls.

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

La actualización de la configuración garantiza tener un inventario de todos los elementos que conforman la red. Además, ayuda a que los cambios o modificaciones que se efectúen estén soportados sobre el estudio previo de las configuraciones existentes, evitando así problemas.

Mapa de red

El mapa de red proporciona el sistema administrador de red y debe ser lo suficientemente potente y amigable como para que permita el manejo de la configuración, además de lograr visualizar a través suyo el punto donde se ha detectado una falla.

Se pueden tener dos tipos de mapas: geográfico y topológico. El mapa geográfico se hace necesario cuando se tienen muchas de redes LAN dispersas e interconectadas. Este tipo de mapa muestra la ubicación geográfica de cada uno de los elementos que componen la red. El mapa topológico, por su parte, sirve para visualizar los dispositivos y enlaces establecidos entre ellos, sin interesar si se encuentran en su posición geográfica exacta. Es muy usado para redes pequeñas. Dependiendo de la magnitud

de la red y de su distribución, se puede usar tanto el uno como el otro, o una combinación de ambos, para obtener mayor claridad de la magnitud de la red.

Manejo de inventarios

Manejo de inventarios está directamente ligado con el mapa de red y con el manejo de la configuración. Su utilidad radica en poder llevar el registro de los equipos que se han utilizado a lo largo del ciclo de vida de la red, lo que arrojará el histórico de su evolución. Se hace útil, igualmente, en caso de tener alguna falla lógica o física en la red reportada por un usuario, ya que rápidamente, a través del inventario, se identifica la configuración de ese punto y se determina si la falla es generada ahí o en otro punto.

Planeación de red

Planeación de red se refiere a las reformas a realizar, 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.

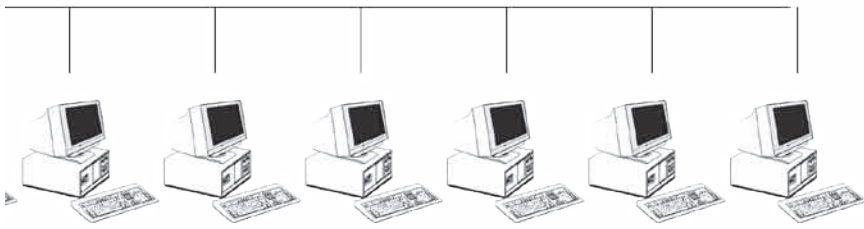
Esta planeación de red debe responder a las necesidades que se van presentando y a la actualización del administrador, para que le permita incorporar nuevos productos y equipos a la red, a fin de mejorar los servicios presentes o implementar nuevos que mejoren la productividad de los usuarios.

Contabilidad de costos

Contabilidad de costos es apropiada en empresas con redes grandes y divididas en departamentos, en donde a cada departamento se le carga el costo de tener la red en funcionamiento. Poner en funcionamiento una red implica una serie de costos, que al inicio son altos y los cuales hay que poner en confrontación con los beneficios obtenidos, buscando que la relación establecida entre estas dos cantidades sea mayor a uno (1).

FMC¹

Control centralizado

Programación *off-line* descentralizada

Desarrollos con red LAN y ambiente virtual:

1. Modelamiento y proyectos de automatización, robots y FMC.
2. Simulación y programación *off-line* de automatización y robots industriales.
3. Simulación y programación *off-line* de sistemas CAD / CAM.
4. Planeamiento estratégico de FMS (*FMS Scheduling*)
5. Robótica avanzada y nuevas aplicaciones industriales.
6. Diseño mecatrónico de robots, dispositivos y mecanismos.
7. Manufactura integrada por computador CIM.

Figura 5. Enseñanza de robótica y FMS en ambiente virtual.

Tendencias

A nivel de las redes de datos, su aplicación en las fábricas y administración, se pueden evidenciar varias tendencias y desarrollo futuros. Dentro de los más relevantes se cuentan:

- Unificar las redes de datos y las redes de los sistemas flexibles de manufactura en un solo sistema que sea totalmente transparente para el usuario. Esto permitirá que las organizaciones puedan tener un único sistema de administración de red que consolide los datos de ambos ambientes.
- Las redes inalámbricas serán la próxima generación de redes en la fábrica. Se está trabajando en codificaciones que sean inmunes al ruido y las interferencias magnéticas.

- Elementos activos cuyo consumo de corriente sea muy bajo o, en el mejor de los casos, que su alimentación se tome directamente del elemento conectante, lo cual ayuda a reducir de tamaño los dispositivos, permitiendo que se integre a los medios generadores de datos.

- Cuando se tiene menor información que transmitir se requiere menos ancho de banda, pero actualmente el flujo de información es creciente, por tal razón se está trabajando en algoritmos que permitan mayores grados de compresión de la información, acción que se hace más necesaria cuando se están transmitiendo imágenes. Esto contribuiría sustancialmente a disminuir el tráfico efectivo de información, pero aumentaría el tráfico de tramas de control.

- Uno de los grandes inconvenientes de la administración de redes es el alto flujo de información que se genera. Por esto, se está trabajando en un concepto denominado agentes inteligentes, los cuales estarían distribuidos por toda la red, monitoreándola continuamente y almacenando la información en bases de datos distribuidas.

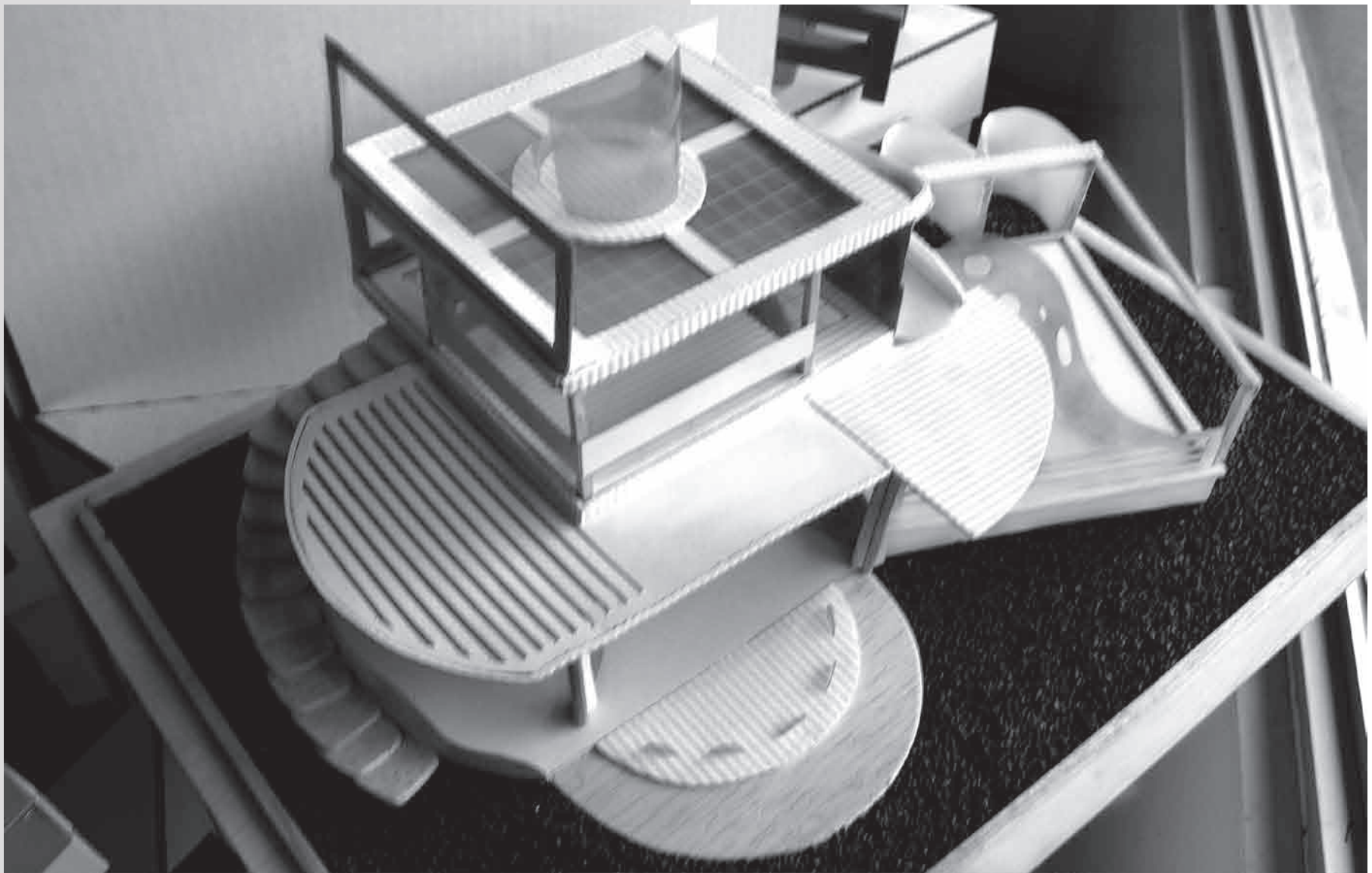
5. Conclusiones

El análisis de tráfico es la principal herramienta que se posee para la administración de redes, ya que a través suyo se identifica la mayoría de fallas e inconvenientes que se presentan en las redes de comunicación de datos.

La administración eficiente de redes de computadores LAN es la integración humana y tecnológica hacia una estrategia de aplicación óptima de los recursos de una empresa. Dicha administración significa aplicar una integración sinérgica de recursos humanos y físicos hacia la productividad, competitividad y flexibilidad de la fábrica, en un mundo cada vez más globalizado.

Es necesario tener en cuenta que a medida que se aumenten los controles de seguridad el redimiendo de la red decrece, por tanto, es necesario tomar medidas complementarias que permitan contrarrestar esta pérdida.

El control de configuración es una de las tareas que un administrador de red debe mantener actualizada y en lo posible automatizada, ya que así puede saber con qué recursos cuenta y le permite dar respuestas eficientes en caso de ser necesario efectuar algún cambio. Cabe recordar que el éxito de las redes radica en el hecho de que el usuario no se percate de su presencia.



Referencias bibliográficas

- Ahuja, Vigía. *Design and analysis of computer communications networks*. Singapore: McGraw Hill, Inc., 1982.
- Carvajal Rojas, Jaime Humberto. "Metodología de Modelagem, Simulação e Programação Off-Line de Robôs e Dispositivos Mecatrônicos Integrados e Direcionados à Células Flexíveis de Manufatura FMC". Ph. D. Trabajo de grado (Ingeniería Mecánica). Brasil: Universidade Estadual de Campinas, 2004.
- Derfler, Frank. *Descubre Redes Lan & Wan. Claro. Conciso. Confiable*. Madrid: Prentice Hall, 1998.
- Hunter, Philip, *Local Area Network, Making the right choice*. Great Britain: Addison-Wesley, 1993.
- McClure, Stuart. *Hackers: Secretos y Soluciones para la seguridad de redes*. España: McGraw Hill, 2000.
- Northcutt, Stephen. *Detección de Intrusos. Guía Avanzada*. 2da. Edición. España: Pearson Educación, 2001.
- Piattini, Mario G., *Auditoría Informática. Enfoque práctico*. México: Alfaomega, 1998.

Notas

- ¹ A esta red se le denominó Ethernet. La figura 1 presenta el plano en borrador de dicha red. Este gráfico fue tomado del sitio de Xerox.
- ² Cabe 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 Figura tomada de la página web: http://www.tcp-ip-info.de/tcp_ip_und_internet/ethernet.gif

⁴ Esta convergencia se propició por el uso cada vez más común de elementos de procesamiento en las comunicaciones -lo cual las iba haciendo más eficientes-, por el proceso de digitalización de todo tipo de información y por la necesidad de compartir información en forma fácil y en tiempo real.

⁵ 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.

⁶ Figura tomada de la página web: http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/images/Observer_bandwidth_utilization_graph.gif

⁷ 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.

⁸ Alguno de los parámetros estadísticos a tener en cuenta pueden ser promedio de paquetes enviados, recibidos, retransmisiones, overhead, tráfico efectivo tasa de errores, entre otros.