Un modelo funcional para la administración de redes

Carlos A. Vicente Altamirano[1]

[1]UNAM - DGSCA
Dirección de Telecomunicaciones, Departamento de Operación de la red
Centro de operación de RedUNAM (NOC-UNAM)
carlos@noc.unam.mx
Julio de 2003

Resumen

Se describe una metodología de redes de datos basada en modelos funcionales estándar de la ITU y de la ISO. Estos modelos detallan las tareas y funciones que deben ser ejecutadas en el proceso de administración de redes.

1. INTRODUCCIÓN

Administración de redes.

El término *administración de redes* es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

Tres dimensiones de la administración de redes.

a) **Dimensión Funcional.** Se refiere a la asignación de tareas de administración por medio de áreas funcionales.
b) **Dimensión Temporal.** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.
c) **Dimensión del escenario.** Se refiere al resto de los escenarios adicionales al de administración de redes, como son administración de sistemas, administración de aplicaciones, etc.

Dimensión Funcional

Existen diversas modelos sobre arquitecturas de administración de redes. Tanto el modelo TMN[1] de la ITU como el modelo OSI-NM[2] (Network Management) son modelos funcionales que dividen la administración de una red en áreas funcionales (configuración, fallas, desempeño, contabilidad y seguridad), definiendo de ésta forma una estructura

organizacional con funciones bien definidas. De esto se deriva el nombre de modelos funcionales.

El presente trabajo se basa únicamente a lo que proponen los modelos funcionales mencionados.

2. DESARROLLO DE LA METODOLOGÍA

Se sugiere la creación de las siguientes áreas funcionales para ser aplicadas en la administración de redes.

2.1. Administración de la configuración

A continuación se describen las actividades ubicadas dentro del proceso de la administración de la configuración. Estas actividades son la planeación y diseño de la red; la instalación y administración del software; administración de hardware, y el aprovisionamiento. Por último se mencionan los procedimientos y políticas que pueden ser de ayuda para el desarrollo de esta área.
.

2.1.1. Planeación y diseño de la red.

La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

El proceso de planeación y diseño de una red contempla varias etapas, algunas son:

a) Reunir las necesidades de la red. Las cuales pueden ser específicas o generales, tecnológicas, cuantitativas, etc. Algunas de las necesidades específicas y de índole tecnológico de una red pueden ser

   - Multicast,
   - Voz sobre IP (VoIP),
   - Calidad de servicio (QoS), etc.

   Algunas necesidades cuantitativas pueden ser

   - Cantidad de nodos en un edificio
   - Cantidad de switches necesarios para cubrir la demanda de nodos.

Este tipo de requerimientos solamente involucran una adecuación en el diseño de la red, no requiere de un rediseño completo, en el caso de alguna necesidad más general puede requerir de un cambio total en la red ya que en estos casos los cambios afectan a gran parte del diseño. Una necesidad general, por ejemplo, se presenta cuando se desea la implementación de nuevas tecnologías de red como el cambiar de ATM a GigabitEthernet, o cambiar los protocolos de ruteo interno.

b) Diseñar la topología de la red

c) Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.

d) Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático o dinámico.

e) Si el diseño y equipo propuesto satisfacen la necesidades, se debe proceder a planear la implementación, en caso contrario, repetir los pasos anteriores hasta conseguir el resultado esperado.

2.1.2. Selección de la infraestructura de red.

Esta selección se debe realizar de acuerdo a las necesidades y la topología propuesta. Si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo (core). Además, la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo mas recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

2.1.3. Instalaciones y Administración del software.

El objetivo de estas actividades es conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

Instalaciones de hardware

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo completo, como un switch o un ruteador; o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc. El proceso de instalación consiste de las siguientes etapas:

- Realizar un estudio previo para asegurar que la parte que será instalada es compatible con los componentes ya existentes.
- Definir la fecha de ejecución y hacer un estimado sobre el tiempo de duración de cada paso de la instalación.
- Notificar anticipadamente a los usuarios sobre algún cambio en la red.
- Generalmente, a toda instalación de hardware corresponde una instalación o configuración en la parte de software, entonces es necesario coordinar esta configuración.
- Generar un plan alterno por si la instalación provoca problemas de funcionalidad a la red.
- Realizar la instalación procurando cumplir con los límites temporales previamente establecidos.

- Documentar el cambio para futuras referencias.

Administración del software.

Es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.
Antes de realizar una instalación, se debe tomar en cuenta lo siguiente.

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.

- Asegurar que no exista conflicto alguno, entre las versiones actuales y las que se pretenden instalar.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requieren especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar las configuración al dispositivo mediante un servidor de tftp.

2.1.4. Provisionamiento

Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware mas importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

- Algunos elementos de hardware más importantes como son: tarjetas procesadoras, fuentes de poder, módulos de repuesto, equipos para sustitución y un respaldo de cada uno de ellos.

2.1.5. Políticas y procedimientos relacionados

En este apartado se recomienda realizar, entre otros, los siguientes procedimientos y políticas.

- Procedimiento de instalación de aplicaciones más utilizadas.

- Políticas de respaldo de configuraciones.
- Procedimiento de instalación de una nueva versión de sistema operativo.

2.2. Administración del rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado.

La administración del rendimiento se divide en 2 etapas: monitoreo y análisis.

2.2.1 Monitoreo

El monitoreo consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

a) *Utilización de enlaces*

Se refiere a las cantidades ancho de banda utilizado por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc), ya sea por elemento o de la red en su conjunto.

b) *Caracterización de tráfico.*

Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son más utilizados. Además, esto también permite establecer un patrón en cuanto al uso de la red.

c) *Porcentaje de transmisión y recepción de información.*

Encontrar los elementos de la red que mas solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.

d) *Utilización de procesamiento*

Es importante conocer la cantidad de procesador que un servidor esta consumiendo para atender una aplicación.

Esta propuesta considera importante un sistema de recolección de datos en un lugar estratégico dentro de la red, el cual puede ser desde una solución comercial como Spectrum o la solución propia de la infraestructura de red, hasta una solución integrada con productos de software libre.

2.2.2 Análisis.

Una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño.

En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

a) *Utilización elevada.*

Si se detecta que la utilización de un enlace es muy alta, se puede tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico. También, el incremento en la utilización, puede ser el resultado de la saturación por tráfico generado maliciosamente, en este caso de debe contar con un plan de respuesta a incidentes de seguridad.

b) *Tráfico inusual.*

El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.

c) *Elementos principales de la red.*

Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con mas actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.

d) *Calidad de servicio.*

Otro aspecto, es la Calidad de servicio o QoS, es decir, garantizar, mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren de un trato especial, como lo son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.

e) Control de tráfico.

El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

Si las acciones tomadas no son suficientes, éstas se deben reforzar para que lo sean, es decir, se debe estar revisando y actualizando constantemente.

2.2.3 Interacción con otras áreas

La administración del rendimiento se relaciona con la administración de fallas cuando se detectan anomalías en el patrón de tráfico dentro de la red y cuando se detecta saturación en los enlaces. Con la administración de la seguridad, cuando se detecta tráfico que es

generado hacia un solo elemento de la red con más frecuencia que la común. Y con la administración de la configuración, cuando ante una falla o situación que atente contra el rendimiento de la red, se debe realizar alguna modificación en la configuración de algún elemento de la red para solucionarlo.

2.3. Administración de fallas

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red. Consiste de varias etapas. Primero, una falla debe ser detectada y reportada de manera inmediata. Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar. Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla. Una vez que el origen ha sido detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

El proceso de la administración de fallas consiste de distintas fases.

- *Monitoreo de alarmas.* Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.

- *Localización de fallas.* Determinar el origen de una falla.

- *Pruebas de diagnóstico.* Diseñar y realizar pruebas que apoyen la localización de una falla.

- *Corrección de fallas.* Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.

- *Administración de reportes.* Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

2.3.1. Monitoreo de alarmas

Las alarmas son un elemento importante para la detección de problemas en la red. Es por eso que se propone contar con un sistema de alarmas, el cual es una herramienta con la que el administrador se auxilia para conocer que existe un problema en la red. También conocido como sistema de monitoreo, se trata de un mecanismo que permite notificar que ha ocurrido un problema en la red. Esta propuesta se basa en la utilización de herramientas basadas en el protocolo estándar de monitoreo, SNMP, ya que este protocolo es utilizado por todos los fabricantes de equipos de red.

Cuando una alarma ha sido generada, ésta debe ser detectada casi en el instante de haber sido emitida para poder atender el problema de una forma inmediata, incluso antes de que el usuario del servicio pueda percibirla.

Las alarmas pueden ser caracterizada desde al menos dos perspectivas, su tipo y su severidad.

Tipo de las alarmas

- *Alarmas en las comunicaciones.* Son las asociadas con el transporte de la información, como las pérdidas de señal.

- *Alarmas de procesos.* Son las asociadas con las fallas en el software o los procesos, como cuando el procesador de un equipo excede su porcentaje normal.

- *Alarmas de equipos.* Como su nombre lo indica, son las asociadas con los equipos. Una falla de una fuente de poder, un puerto, son algunos ejemplos.

- *Alarmas ambientales.* Son las asociadas con las condiciones ambientales en las que un equipo opera. Por ejemplo, alarmas de altas temperaturas.

- *Alarmas en el servicio.* Relacionadas con la degradación del servicio en cuanto a límites predeterminados, como excesos en la utilización del ancho de banda, peticiones abundantes de icmp.

Severidad de las alarmas.

- *Crítica.* Indican que un evento severo ha ocurrido, el cual requiere de atención inmediata. Se les relaciona con fallas que afectan el funcionamiento global de la red. Por ejemplo, cuando un enlace importante está fuera de servicio, su inmediato restablecimiento es requerido.

- *Mayor.* Indica que un servicio ha sido afectado y se requiere su inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.

- *Menor.* Indica la existencia de una condición que no afecta el servicio pero que deben ser tomadas las acciones pertinentes para prevenir una situación mayor. Por ejemplo, cuando se alcanza cierto límite en la utilización del enlace, no indica que el servicio sea afectado, pero lo será si se permite que siga avanzando.

- *Indefinida.* Cuando el nivel de severidad no ha sido determinado por alguna razón.

2.3.2. Localización de fallas.

Este segundo elemento de la administración de fallas es importante para identificar las causas que han originado una falla. La alarma indica el lugar del problema, pero las pruebas de diagnóstico adicionales son las que ayudan a determinar el origen de la misma. Una vez identificado el origen, se tienen que tomar las acciones suficientes para reparar el daño.

Pruebas de diagnóstico

Las pruebas de diagnóstico son medios importantes para determinar el origen de una falla. Algunas de estas pruebas de diagnóstico que se pueden realizar son:

- *Pruebas de conectividad física.*

  Son pruebas que se realizan para verificar que los medios de transmisión se encuentran en servicio, si se detecta lo contrario, tal vez el problema es el mismo medio.

- *Pruebas de conectividad lógica.*

  Son pruebas que ofrecen una gran variedad, ya que pueden ser punto a punto, o salto por salto. Las pruebas punto a punto se realizan entre entidades finales, y las salto por salto se realizan entre la entidad origen y cada elemento intermedio en la comunicación. Los comandos usualmente utilizados son “ping” y “traceroute”.

- *Pruebas de medición.*

  Esta prueba va de la mano con la anterior, donde, además de revisar la conectividad, se prueban los tiempos de respuesta en ambos sentidos de la comunicación, la pérdida de paquetes, la ruta que sigue la información.

2.3.3. Corrección de fallas.

Es la etapa donde se recuperan las fallas, las cuales pueden depender de la tecnología de red. En esta propuesta solo se mencionan las prácticas referentes a las fallas al nivel de la red.

Entre los mecanismos más recurridos, y que en una red basada en interruptores son aplicables, se encuentran los siguientes.

- *Reemplazo de recursos dañados. Hay equipos de red* que permiten cambiar módulos en lugar de cambiarlo totalmente.

- *Aislamiento del problema.* Aislar el recurso que se encuentra dañado y que, además, afecta a otros recursos es factible cuando se puede asegurar que el resto de los elementos de la red pueden seguir funcionando.

- *Redundancia.* Si se cuenta con un recurso redundante, el servicio se cambia hacia este elemento.

- *Recarga del sistema.* Muchos sistemas se estabilizan si son reiniciados.

- *Instalación de software.* Sea una nueva versión de sistema operativo, una actualización, un parche que solucione un problema específico, etc.

- *Cambios en la configuración.* También es algo muy usual cambiar algún parámetro en la configuración del elemento de la red.

2.3.4. Administración de reportes

Es la etapa de documentación de las fallas. Cuando un problema es detectado o reportado, se le debe asignar un número de reporte para su debido seguimiento, desde ese momento un reporte queda abierto hasta que es corregido. Este es un medio para que los usuarios del servicio puedan conocer el estado actual de la falla que reportaron.

El ciclo de vida de la administración de reportes se divide en cuatro áreas, de acuerdo a la recomendación X.790 de la ITU-T.

Creación de reportes

Un reporte es creado después de haber recibido una notificación sobre la existencia de un problema un problema en la red, ya sea por una alarma, una llamada telefónica de un usuario, por correo electrónico o por otros medios. Cuando se crea un reporte de be contener al menos la siguiente información:

- El nombre de la persona que reportó el problema
- El nombre de la persona que atendió el problema o que creó el reporte del mismo.
- Información técnica para ubicar el área del problema
- Comentarios acerca de la problemática.
- Fecha y hora del reporte

Seguimiento a reportes

La administración de reportes debe permitir al administrador dar seguimiento de cada acción tomada para solucionar el problema, y conocer el estado histórico y actual del reporte. Para cada reporte debe mantenerse un registro de toda la información relacionada al mismo: pruebas de diagnóstico, como fue solucionado el problema, tiempo que llevó la solución, etc, y esta debe poder ser consultada en cualquier momento por el administrador.

Manejo de reportes

El administrador debe ser capaz de tomar ciertas acciones cuando un reporte está en curso, como escalar el reporte, solicitar que sea cancelado un reporte que no ha sido cerrado aún, poder hacer cambios en los atributos del reporte, como lo es el teléfono de algún contacto, poder solicitar hora y fecha de la creación o finalización de un reporte, etc.

Finalización de reportes

Una vez que el problema reportado ha sido solucionado, el administrador o la gente responsable del sistema de reportes, debe dar por cerrado el reporte. Una práctica importante, es que antes de cerrar un reporte el administrador debe asegurarse que efectivamente el problema reportado ha sido debidamente corregido.

2.4. Administración de la contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

2.5. Administración de la seguridad

Su objetivo es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, así como para la respuesta ante incidentes de seguridad.

2.5.1. Prevención de ataques

El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso. Obviamente, los ataques solamente se reducen pero nunca se eliminan del todo.

2.5.2. Detección de intrusos

El objetivo es detectar el momento en que un ataque se esta llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmes que indiquen el momento en que se detecte una situación anormal en la red.

2.5.3. Respuesta a incidentes

El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema que es parte de la red, cuando éste hay sido detectado, además de tratar de eliminar dichas causas.

2.5.4. Políticas de Seguridad

La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida. Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta tarea debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.

Entre otras, algunas políticas necesarias son:

- Políticas de uso aceptable
- Políticas de cuentas de usuario
- Políticas de configuración de ruteadores
- Políticas de listas de acceso
- Políticas de acceso remoto.
- Políticas de contraseñas.
- Políticas de respaldos.

2.5.5. Servicios de seguridad

Los servicios de seguridad definen los objetivos específicos a ser implementados por medio de *mecanismos de seguridad.* Identifica el "*que".*

De acuerdo a la Arquitectura de Seguridad OSI, un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad :

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Un paso importante es definir cuáles de estos servicios deben ser implementados para satisfacer los requerimientos de las políticas de seguridad.

2.5.6. Mecanismos de seguridad

Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad. Algunas herramientas comunes son: herramientas de control de acceso , cortafuegos (firewall), TACACS+ o RADIUS; mecanismos para acceso remoto como Secure shell o IPSec; Mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

2.5.7. Proceso.

Para lograr el objetivo perseguido se deben, al menos, realizar las siguientes acciones:

- Elaborar las políticas de seguridad donde se describan las reglas de administración de la infraestructura de red. Y donde además se definan las expectativas de la red en cuanto a su buen uso, y en cuanto a la prevención y respuesta a incidentes de seguridad.

- Definir, de acuerdo a las políticas de seguridad, los servicios de necesarios y que pueden ser ofrecidos e implementados en la infraestructura de la red.

- Implementar las política de seguridad mediante los mecanismos adecuados.

3. CONCLUSIONES

La administración de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades hay diferentes responsabilidades fundamentales como el monitoreo, la atención a fallas, configuración, la seguridad, entre otras.

Esto nos lleva a reconocer que una red debe contar con un sistema de administración aun cuando se crea que es pequeña, aunque es cierto que entre mayor sea su tamaño mas énfasis se debe poner en esta tarea.

En los puntos anteriores se describió una propuesta de administración para redes de datos. La propuesta se basó en la recomendación de la ITU-T, el modelo TMN y en el modelo OSI-NM de ISO. Se presentó una propuesta global que enfatiza en todos los aspectos relacionados a la buena operación de una red, como lo son el control sobre los sucesos en la red, la visualización de los tipos de tráfico, la detección y atención oportuna de problemas, aspectos de seguridad, etc.

La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación y actualización.

4. REFERENCIAS

[1]. *Serie de recomendaciones M.3000 de la ITU-T.* http://www.itu.int

[2]. *ISO/IEC 7498-4: 1989.*

[3]. *CAIDA.* http://www.caida.org

5. BIBLIOGRAFIA

- Wang, Henry H. *Telecommunications Network Management.* McGraw-Hill, 1999.
- Hegering, Heinz-Gerd. I*ntegrated Network and System Management Network Management.* Addison-Wesley, 1994.
- Black, Uyless D. *Network management standards : SNMP, CMIP, TMN, MIBs, and object libraries.* Segunda Edición. New York: McGraw-Hill, 1995.
- Kauffels, Franz. *Network Management: Problems, Standards and Strategies.* Addison-Wesley, 1992.
- Tittel, Ed. *Network Design Essentials.* Boston: AP Professional, 1994
- Stallings, William. *Local and Metropolitan Area Networks.*