UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"Metodología para el diseño de redes LAN de alto desempeño en la UNAM"

T E S I S

QUE PARA OBTENER EL TITULO DE:
INGENIERA EN COMPUTACIÓN

PRESENTA:
ALVARO CRUZ CRUZ

ASESOR
ING. JUAN GASTALDI PEREZ

MÉXICO, D.F., 2003

PAGINACION

DISCONTINUA

Agradezco:

A mi mamá, su convicción, valor y fortaleza para formarme e impulsarme hacia nuevos objetivos. Sé que con su experiencia, ejemplo y cualidades, me ha proporcionado todas las herramientas necesarias que para mí son invaluables porque siempre permanecerán conmigo.

A mis tíos y tías, por la importancia que ha tenido en nosotros todo el apoyo que hemos recibido y que ha sido relevante para alcanzar los logros obtenidos

A Rocío, mi novia, cuya presencia ha sido un estímulo constante para crecer juntos, mejorar como seres humanos y encontrar la diversión en cada momento de nuestra vida.

Al Ing. Juan Gastaldi por haber aceptado participar en este proyecto tan importante para mí, aportando sus conocimientos y vocación de enseñanza, así como a los profesores Manuel Quintero, Marcelo Pérez, Moisés Terán y Fernando Márquez por su colaboración y buena disposición para el termino satisfactorio de mi trabajo de tesis.

A todos mis amigos y compañeros por la amistad que me han brindado, siendo parte de experiencias agradables y reconfortantes.

Alvaro

TABLA DE CONTENIDO

Introducción

La necesidad por comunicarse nunca antes ha sido tan grande. Varias instituciones educativas ahora confían en sus redes locales para lograr la comunicación esencial para sus actividades de forma rápida y efectiva; y con una distribución más extensa de aspectos como la información y la educación, la demanda de redes de alto desempeño está creciendo.

Últimamente se ha visto el desarrollo de computadoras personales y servidores más robustos, equipo de comunicaciones y las aplicaciones que pueden hacer uso de todo este poder disponible. Dado que muchas de esas aplicaciones están diseñadas para conectarse a la red, los usuarios están demandando tecnologías LAN de alta velocidad a precios razonables que puedan mantener la tranquilidad en sus aplicaciones de cómputo distribuido. Afortunadamente, o desafortunadamente, dependiendo del punto de vista, en los años recientes se ha visto el desarrollo de un sinnúmero de nuevas tecnologías capaces de proveer servicios de gran capacidad directamente al escritorio. El desarrollo de nuevos equipos de comunicaciones ha permitido a muchas de las redes con falta de buenos niveles de rendimiento actualizarse, simplemente conectando el equipo de red existente a los nuevos, proporcionando una mejora substancial en sus actividades. Por estas razones, es obvio que la calidad de las nuevas redes —la infraestructura de comunicaciones que soporta a una institución— es una parte importante a considerar. Al tener el conocimiento para explotar las nuevas tecnologías es posible satisfacer las necesidades y, en consecuencia, maximizar las probabilidades de éxito.

Generalmente, cada nuevo diseño trae consigo problemas no previstos, que no pueden ser resueltos adecuadamente a la misma velocidad con que surgen las necesidades. Esto puede resultar en redes que son difíciles de entender y mantener. También pueden generar redes que no se desempeñan como lo esperado, no se adaptan al crecimiento y no concuerdan con las necesidades de los usuarios. Una solución a este problema es utilizar una metodología de diseño sistemática que se enfoque en los requerimientos y objetivos del usuario.

Un diseño de red adecuado debe reconocer que los requerimientos del usuario abarcan aspectos como la disponibilidad, confiabilidad, escalabilidad, seguridad y con todo esto, ser administrable. La metodología para el diseño de redes de alto desempeño está basada en la máxima de que el diseño debe comenzar de las capas superiores del modelo de referencia OSI antes de pasar a las capas inferiores.

El proceso de diseño incluye el análisis de las necesidades de red de cada una de las áreas que componen la estructura organizacional, la gente a la cual la red va a servir y de la que se va a obtener información valiosa para que el diseño sea exitoso.

Para evitar inundarse de detalles demasiado rápido, es importante obtener una visión general de los requerimientos del usuario. Posteriormente, puede definirse el uso de protocolos, la escalabilidad, las preferencias tecnológicas, etc. El diseño de redes de alto desempeño, toma en cuenta que el diseño lógico y físico puede cambiar conforme aumente la cantidad de información obtenida en cada una de las etapas.

Es la metodología para el diseño de redes LAN de alto desempeño lo que el presente trabajo pretende abordar, mostrando técnicas de diseño ilustradas con ejemplos, utilizando la experiencia acumulada de muchas personas en la UNAM, proyectos, redes y la mía propia.

Para ello, en el capítulo 1 se expone un síntesis de los orígenes de Internet, y como se ha integrado a la vida académica de la UNAM hasta convertirse en parte fundamental para su desarrollo. Es importante el repaso de los antecedentes históricos específicos de la UNAM, porque la ubican en los cambios descritos y dan una visión del papel que juega en la sociedad. También es importante hacer notar el rol que tienen las instituciones y así comprender porqué cada una presenta cierta independencia y debe ser tratada como un ente con mecanismos y necesidades propios. Esto último, aplicado al tema concerniente al trabajo presentado, marca la pauta para dedicar gran parte del tiempo al diseño de redes individuales capaces de interactuar en conjunto sin afectarse mutuamente. Para sentar las bases del trabajo presentado se ofrece una introducción a las redes de alto desempeño junto con las áreas involucradas, como son las telecomunicaciones, el cómputo y el trabajo del diseñador de este tipo de redes.

En el capítulo 2 se trata a detalle la metodología para el diseño de redes de alto desempeño, basándose en una serie de pasos sistemáticos que deben ser completados, estableciendo un punto de partida y el objetivo final. Con un proyecto a gran escala, el trabajo del diseñador puede ser dividido en varias áreas de trabajo, mismas que son listadas y explicadas. Sin embargo existen tres áreas que merecen ciertas anotaciones al respecto. Una de ellas es la labor de recabar y documentar las necesidades, para lo cual se requiere que el diseñador platique con las personas que realmente utilizan los servicios y que verdaderamente refleje sus necesidades. También debe proveer un diseño con la suficiente flexibilidad y agilidad para evolucionar y satisfacer los constantes cambios; y por último, la verificación, validación y pruebas, que deben ser asociadas con todas las etapas del diseño. Este es el nivel de detalle que se requiere para una metodología de diseño de redes LAN de alto desempeño.

En el capítulo 3 se exploran algunas consideraciones para el diseño físico y lógico. La importancia de este capítulo recae en el hecho de que la UNAM cuenta con una variedad de tecnologías involucradas en su funcionamiento, por lo que se presenta un repaso de las características generales de las redes de área local y las redes a gran escala. Al mismo tiempo se tratan las tecnologías de transporte y los esquemas de direccionamiento y ruteo mas utilizados en la Universidad. Es importante recalcar que en el trabajo presentado no se propone el cambio hacia nuevas tecnologías o lo adquisición de nuevo equipamiento como única opción, por el contrario, se proponen cambios con los recursos existentes. En varias ocasiones no es tan necesario la adquisición de lo último en tecnología si no se van a aprovechar todas las características que justifican el precio del producto, basta con modificar la topología de la red para tener muy buenos resultados.

En el capítulo 4 se ejemplifican casos reales tomados del trabajo diario en el área de atención y solución a fallas en RedUNAM. La metodología mostrada en el capítulo 2 puede ser llevada a cabo, con el apoyo necesario, por los responsables de cómputo. Sin embargo al finalizar dicha tarea probablemente se piense que el siguiente paso obligado es la adquisición de nuevo equipo activo de comunicaciones. Es en esta etapa en donde se remarca la importancia del capítulo cuarto, mostrando como se puede mejorar el desempeño de una red sin que la falta de recursos económicos sea una limitante, empleando, en la medida de lo posible, el equipo existente.

Los cuatro capítulos han sido desarrollados con apego al rumbo que han tomado las redes en la UNAM, no solo en cuanto a tecnología, también en cuanto a la comunidad de usuarios y la forma en que aprovechan los recursos disponibles. Se han tratado de seleccionar los temas mas importantes y los casos mas representativos, esperando que sean de gran ayuda para la comunidad responsable de dirigir los pasos de la Universidad en el diseño de redes.

Capítulo 1. Antecedentes

En un mundo dominado por las comunicaciones, las redes son la clave, ya que proveen el sistema nervioso a cualquier sistema de información para ser eficaz.

Las redes que satisfacen todas las necesidades son grandes y complejas. Muchos de nosotros todavía utilizamos el teléfono como nuestro principal medio de comunicación, transmisiones de fax ilegibles, viajamos a las reuniones y sufrimos para las transferencias vía correo electrónico. Esto deja dos mensajes: el primero es que las redes de alto desempeño no son ya opcionales, se están convirtiendo en parte esencial para muchas operaciones. El segundo mensaje es que la conciencia de sus ventajas no está muy arraigada por lo que muchas redes siguen simplemente creciendo en lugar de ser apropiadamente diseñadas.

1.1. Internet

El Internet ha revolucionado el mundo de la computación y las comunicaciones como nunca antes se había visto. La invención del telégrafo, el teléfono, el radio y la computadora marcaron la pauta para la integración, sin precedentes, de casi cualquier tipo de servicio. Es por si mismo un mundo lleno de capacidades, un mecanismo para la diseminación de información, y un medio para que la colaboración y la interacción entre individuos y sus computadoras suceda independiente de su localización geográfica.

El Internet representa uno de los mejores ejemplos acerca de los beneficios que tienen la dedicación y la constancia al investigar y desarrollar la infraestructura para el intercambio de información. A partir de los primeros estudios sobre la conmutación de paquetes: el gobierno, la industria y la educación han colaborado para promover esta nueva tecnología, en donde su rápido crecimiento se debe en gran medida al acceso libre y sin restricciones a los documentos relacionados, especialmente a los que especifican el uso de los protocolos. Hoy día, términos como "usuario@servidor.unam.mx" y "http://www.unam.mx" son comunes escucharlos en las conversaciones.

La historia del Internet circunda alrededor de cuatro aspectos fundamentales [bib01]:

- La evolución tecnológica que comenzó con el desarrollo de la conmutación de paquetes y que continúa investigándose con el fin de expander los horizontes en varias direcciones, como el dimensionamiento, rendimiento y altos niveles de funcionalidad.
- La operación y la administración de su compleja infraestructura.
- El aspecto social, que resulta en una comunidad que colabora para crear e impulsar la tecnología.
- El aspecto comercial, que permite una transición extremadamente efectiva hacia nuevas tecnologías.

1.1.1. Orígenes de Internet

El primer registro que describe la interacción entre individuos a través de una red fueron una serie de memorándums escritos por J.C.R. Licklider en agosto de 1962, en los cuales se divulgaba el concepto de "Red Galáctica". El visualizó un grupo de computadoras globalmente interconectadas para que cualquier persona pudiera, rápidamente, tener acceso a programas e información independiente de su ubicación geográfica.

Un concepto crucial fué que el sistema tenía una arquitectura abierta, de hecho la idea original de Licklider de una "Red Galáctica" fué:

- Cada red debe ser capaz de trabajar por si misma, desarrollando sus propias aplicaciones sin restricciones y sin requerir modificaciones para participar en la red.
- Dentro de cada red habrá un gateway, el cual la enlazará con el mundo exterior. Esto puede ser una gran computadora (capaz de manejar el volumen de tráfico) con el software necesario para transmitir y redireccionar cualquier paquete.

- El gateway no retendrá información acerca del tráfico que pasa a través de él. Será diseñado para disminuir la carga de trabajo y dar mayor velocidad al flujo de tráfico; también removerá posibles fuentes de censura y control.

- Los paquetes deberán ser reenviados a través de la ruta más rápida disponible. Si una computadora es bloqueada o lenta, los paquetes serán reenviados por la nueva ruta hasta que eventualmente alcancen su destino.

- Los gateways entre las redes siempre deberán estar abiertos, y reenviarán el tráfico sin discriminación.

- Los principios de operación deberán estar gratuitamente disponibles a todas las redes.

En esencia, el concepto hace referencia a lo que es Internet actualmente y los escritos de Licklider comenzaron a hacerse realidad a partir de dos sucesos importantes: La publicación de la teoría de la conmutación de circuitos en julio de 1961 por Leonard Kleinrock y la interconexión de las primeras dos computadoras en una red de área amplia a través de una línea telefónica. El experimento permitió establecer que las computadoras podían trabajar correctamente compartiendo recursos para ejecutar programas e intercambiar información con la máquina remota. Para finales de 1969, cuatro computadoras fueron conectadas a la naciente ARPANET, y con esto despegó el Internet [bib01]. En octubre de 1972 se organizó la primera demostración pública de la tecnología ARPANET y fue en marzo del mismo año cuando la primera aplicación, el correo electrónico, apareció, a partir de la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo para coordinarse. En julio, se mejoró la primer versión del programa añadiéndole utilidades como listar, seleccionar mensajes, agregar archivos, reenviar y responder mensajes.

La motivación inicial para el surgimiento de ARPANET e Internet fue la compartición de recursos – por ejemplo, permitir a distintos usuarios el acceso a varios dispositivos compartidos conectados a ARPANET, en lugar de duplicar computadoras costosas e información. Sin embargo, mientras que la transferencia de archivos (FTP) y el acceso remoto (Telnet) fueron aplicaciones verdaderamente importantes, el correo electrónico tendría quizá el impacto más significativo dentro de las innovaciones de ésa era. El correo electrónico proporcionó un nuevo modelo de como las personas podían comunicarse entre sí, y cambió la naturaleza de la comunicación, primero entre los involucrados en el desarrollo de Internet y después en la sociedad. A partir de ahí se consideró al correo electrónico como la aplicación de red más difundida por toda una década, premonición de lo que actualmente consideramos para el World Wide Web.

En diciembre de 1970, el NWG (Network Working Group) finalizó la construcción del primer protocolo máquina-a-máquina, llamado NCP (Network Control Protocol) y de esta forma los usuarios de red finalmente comenzaron a desarrollar aplicaciones. En 1973, U.S.DARPA (U.S. Defense Advanced Reserch Projects Agency) inició un programa de desarrollo con el fin de investigar técnicas y tecnologías para interconectar redes paquetizadas. El objetivo era desarrollar un protocolo de comunicaciones que permitiera a las computadoras conectadas a la red comunicarse transparentemente a través de múltiples redes. Este proyecto fue llamado "*Internetting*" y el sistema de redes que emergió de dicha investigación se conoció como Internet.

Posteriormente, se presentó una nueva versión que reunía las necesidades para un ambiente de red de arquitectura abierta. Eventualmente, este protocolo se llamó TCP/IP (Transmition Control Protocol/Internet Protocol). Mientras que NCP estaba diseñado para funcionar como un dispositivo controlador, la nueva versión pretendía funcionar como un protocolo de comunicaciones. Hubo otras propuestas de aplicaciones en los primeros días de Internet, incluyendo voz paquetizada (precursor de voz por IP), varios modelos para compartir archivos y almacenamiento, y los primeros programas que mostraron el concepto de agentes (y por supuesto, virus). Un concepto fundamental de Internet es que no fue diseñado para una sola aplicación, pero si como una estructura general en la cual nuevas aplicaciones pudieran ser concebidas, como podría ser el World Wide Web. Y todo esto impulsado por el servicio que proporcionaban TCP e IP.

Al mismo tiempo se comenzó a definir el concepto de "Red de arquitectura abierta" dictando que las redes individuales podían ser diseñadas de acuerdo a necesidades específicas e inclusive contar con interfaces únicas que ofrecer a los usuarios y a otros proveedores. Sin embargo, a pesar de que no había restricciones en los tipos de redes a implantar, si existían consideraciones que dictaban lo que era razonable ofrecer (proyecto

Internetting). Las redes fueron surgiendo (incluyendo ARPANET) acorde a propósitos específicos, por ejemplo, en 1980-81 se dio inicio a los proyectos BITNET Y CSNET. BITNET apegado a una naturaleza multidisciplinaria con usuarios de todas las áreas académicas, mientras que CSNET se fundó para proveer interconexión a grupos de investigación ubicados en las universidades, industria y gobierno. British JANET (1984) y U.S. NSFNET (1986) fueron programas que anunciaron explícitamente su interés por atender a comunidades estudiantiles, independiente de la disciplina, es más, uno de los requisitos para que una universidad tuviera acceso a NSFNET era que la conexión estuviera disponible a todo aquel usuario calificado en el cámpus.

Obviamente, existía la necesidad de que fueran compatibles entres ellas y desafortunadamente no lo eran, aunado a las tecnologías alternas que hicieron su aparición en el sector comercial, incluyendo XNS de Xerox, DECNet, y SNA de IBM.

CSNET fue inicialmente fundada por el NSF (National Foundation Science) para proveer la interoperatividad en las universidades, industria y los grupos gubernamentales de investigación en la ciencia del cómputo. CSNET fue pionera en el uso de TCP/IP sobre X.25 usando redes públicas comerciales de datos. El servidor de nombres CSNET proporcionó un primer ejemplo de un servicio de directorio.

En 1987, BITNET y CSNET se fusionaron para formar el CREN (Corporation for Research and Educational Networking). En 1991, el servicio CSNET fue descontinuado habiendo completado su importante rol de aprovisionamiento de un servicio de interoperatividad académica. Una característica clave de CREN es que sus costos operacionales son completamente financiados a través del pago de cada una de sus organizaciones miembros.

En 1986, el U.S.NSF (United States National Science Foundation) inició el desarrollo de NSFNET, el cuál, hoy día, provee un importante backbone de servicios de comunicación para Internet. Con facilidades como 45 megabits por segundo, NSFNET transporta alrededor de 12 billones de paquetes por mes entre las redes que enlaza. La NASA (National Aeronautics and Space Administration) y el U.S.DE (United States Department of Energy) contribuyen con facilidades adicionales de backbone en la forma de NSINET y ESNET respectivamente. En Europa, importantes backbones internacionales como NORDUNET y otros proveen conectividad a más de cien mil computadoras en un gran número de redes. Los proveedores de redes comerciales están comenzando a ofrecer backbone de Internet y soporte para el acceso sobre una base competitiva para cualquier interesado.

Durante el curso de su evolución, particularmente después de 1989, el sistema de Internet comenzó a integrar el soporte para otros protocolos, mediante dispositivos de interconexión, dentro de su configuración básica de fábrica. El énfasis principal del sistema es el desempeño multiprotocolo, y en particular, con la integración de los protocolos OSI (Open Systems Interconnection) dentro de la arquitectura.

A pesar de que Ethernet se encontraba en desarrollo en Xerox PARC, la proliferación de LAN's no se vislumbraba, mucho menos las computadoras personales y estaciones de trabajo. El modelo original de redes fue de tipo nacional como ARPANET, de las cuales se esperaba que su número fuera pequeño, por lo que se utilizaron direcciones IP de 32 bits con los primeros 8 bits como identificadores de la red y los 24 bits restantes como identificadores del usuario en la red [bib01]. La idea de que 256 redes serían suficientes para el futuro, tuvo que ser reconsiderada cuando comenzaron a aparecer las LAN a finales de 1970, siendo a mediados de los 80's que el desarrollo de LAN's, PC's y estaciones de trabajo formarían el impulso necesario para el crecimiento de Internet.

Ethernet es probablemente la tecnología de red predominante en Internet y PC's y estaciones de trabajo las computadoras dominantes. Este cambio de tener pocas redes con usuarios compartiendo recursos (ARPANET) a tener muchas redes ha resultado en conceptos nuevos y modificaciones a la tecnología original. Primero resultó en la definición de tres clases de redes (A, B, y C) para dar cabida al rango de usuarios. La clase A representa grandes redes de dimensiones nacionales (pocas redes con muchos usuarios); la clase B representa redes de escala regional; y la clase C representa redes locales (muchas redes con pocos usuarios). Otro cambio importante fue la asignación de nombres a usuarios para hacer más práctico el trabajo con redes y evitar tener que recordar direcciones numéricas. Originalmente, cuando el número de usuarios era

pequeño, resultó fácil administrar una tabla de usuarios relacionando nombre y dirección. El cambio a tener un número bastante grande de redes independientes (LAN) complicaba el uso de una sola tabla, y por este motivo se inventó el DNS (Domain Name System), siendo su introducción oficial en 1984. El nuevo sistema introdujo cierta nomenclatura en las direcciones de Internet de Estados Unidos, como edu. (educational), com. (commercial), gov. (governmental) además de org. (international organization) y una serie de códigos de país como .mx (México), .ca (Canadá), .us (Estados Unidos), etc. El DNS permitió un mecanismo de distribución escalable para resolver nombres de usuarios jerárquicos (ej. www.unam.mx) a direcciones IP.

El incremento en el tamaño de Internet también puso un reto para las capacidades de los routers y los procedimientos para administrar la red. Originalmente existía un sólo algoritmo para ruteo que fue implementado uniformemente por todos los routers conectados a Internet, mismo que requería de configuración manual de tablas de ruteo; posteriormente fue reemplazado por algoritmos automáticos de distribución y mejores herramientas diseñadas para solucionar fallas. Conforme el número de redes en Internet creció, el diseño inicial no pudo hacerlo a la par, así que fue reemplazado por un modelo jerárquico de ruteo con un protocolo interior, IGP (Interior Gateway Protocol), utilizado dentro de cada región de Internet, y un protocolo exterior, EGP (Exterior Gateway Protocol), utilizado para concatenar regiones. Este diseño permitía la instalación de diferentes versiones de IGP dependiendo de parámetros como: costo, configuración, adaptabilidad, modularidad, etc. En 1987 se volvió claro que se requería de un protocolo que permitiera que elementos de la red, como routers, pudieran ser administrados de manera remota y uniforme. De esta manera, varios protocolos fueron propuestos, de los cuales SNMP es el de mayor uso actualmente.

El backbone realizó la transición de una red basada en routers diseñados por los propios investigadores a equipo enteramente comercial. A partir de 1987, el backbone creció de seis nodos con enlaces de 56 Kbps a 21 nodos con enlaces múltiplos de 45 Mbps. Internet ha crecido en más de 50,000 redes en los siete continentes y aproximadamente 201 millones de usuarios en todo el mundo, de los cuales 114 millones utilizan el servicio WWW, cifra que va aumentando cada día. La taza anual de crecimiento de usuarios es del 65% [bib17].

El Internet es una colección de comunidades así como una colección de tecnologías, y su éxito se atribuye en gran medida a satisfacer ambas necesidades. Este espíritu de colaboración tiene sus orígenes en la creación de ARPANET, cuando los investigadores tenían que trabajar de manera conjunta para impulsar la tecnología de la conmutación de paquetes. Al igual que otras ramas de investigación, las actividades tenían que ser coordinadas entre miembros de distinta procedencia empleando todos los mecanismos disponibles, comenzando con el correo electrónico, después compartiendo recursos, accesos remotos y, eventualmente, el World Wide Web.

A finales de 1970, se reconoció que el crecimiento de Internet iba de la mano con el crecimiento de comunidades interesadas en formar parte del grupo de investigación. Así pues, los mecanismos de coordinación tenían que ser debidamente definidos y se formaron varios comités. De esta manera, a través de dos décadas de actividad en Internet, se ha visto una constante evolución en las estructuras organizacionales, diseñas para soportar y facilitar a la continuamente creciente comunidad, su trabajo de colaboración en los aspectos relacionados al Internet.

El Internet se ha convertido en un servicio de "comodidad", pues mucha de la atención que ha recibido es en usar esta infraestructura global para soportar casi todo tipo de servicios comerciales. En mayor parte, esto ha sido por la distribución a gran escala de navegadores y de la tecnología World Wide Web, permitiendo a los usuarios un fácil acceso a un mercado creciente de sofisticados servicios de información.

Internet ha cambiado mucho en las dos décadas posteriores a su nacimiento. Fue concebido en la era de la compartición de recursos, pero ha sobrevivido en la era de las computadoras personales, configuraciones cliente-servidor, comunicaciones punto-a-punto y redes de computadoras. Fue diseñado antes de que las redes locales existieran, pero ha acomodado esa tecnología así como al ATM y los servicios de conmutación de paquetes. Fue preparado para soportar varias funciones como compartir información y acceso remoto hasta compartir recursos y colaboración, así como impulsor del correo electrónico y recientemente el WWW. Pero lo más importante, comenzó para ser utilizado por un pequeño grupo de dedicados investigadores, y ha crecido como todo un suceso comercial que genera millones de dólares anualmente.

Sin embargo, no se puede concluir que el Internet ha dejado de crecer, pues se ha convertido en una criatura hecha a base de computadoras, y como tal, continuará cambiando y evolucionando a la velocidad de la industria de la computación. Ahora se está transformando para proporcionar servicios en tiempo real como audio y video. Las capacidades presentadas por Internet, junto con la nueva tecnología portable (ej. Lap-top, localizadores, PDA's, teléfonos celulares) están haciendo posible un nuevo paradigma sin precedentes en la computación y las comunicaciones. Esta evolución nos trae nuevas aplicaciones como telefonía y televisión por Internet. También permitirá formas más sofisticadas para lograr un mejor costo beneficio, quizá uno de los factores más críticos en este comercio. La pregunta más importante respecto al futuro de Internet no es como la tecnología va a cambiar, sino como manejar esos procesos de cambio y evolución. Históricamente, la arquitectura de Internet ha sido dirigida por un grupo de diseñadores, pero esa forma ha cambiado a partir de que el número de interesados con poder económico y conocimientos ha crecido. Ahora se está tratando de definir la nueva generación de direcciones IP y la nueva estructura social que guiara al Internet en el futuro.

1.2. Educación superior en México

Hay que empezar por ubicar el asunto de la educación superior, y en particular de las universidades, en el contexto de la llamada era del conocimiento, y para ello es necesario referirse, por lo menos, a dos de los fenómenos que la condicionan: la globalización y la revolución tecnológica, sobre todo la vinculada a las nuevas tecnologías de información.

La globalización no es un fenómeno nuevo; ha estado siempre acompañada de una transformación en los sistemas de comunicaciones entre los seres humanos y de nuevos descubrimientos, que han permitido transitar a etapas sucesivas en la historia. En esas etapas, ha habido un proceso permanente de globalización y una incesante revolución tecnológica: de la vela a la máquina de vapor, del transporte terrestre al aéreo, del hilo telefónico a la comunicación inalámbrica, y ahora se vive la información en tiempo real. Se sabe lo que pasa en el mundo al momento en que está sucediendo, instantáneamente. Esto es lo que mejor define al fenómeno de la globalización actual, que, además, trasciende los aspectos estrictamente económicos, influye en la política, afecta la cultura y modifica la vida social.

Por otro lado, ocurre que la revolución tecnológica plantea problemas realmente complejos. Un buen ejemplo es el de la competitividad internacional. Quien no se adapta con rapidez a los cambios tecnológicos mediante un proceso permanente de reconversión y reestructuración, queda fuera del mercado. Esto puede ser catastrófico en una época en la cual ya no es posible cerrar las fronteras, por lo que es necesario encontrar soluciones a dichos problemas y hacer el propósito de sacar el mayor provecho posible tanto de la globalización como de la revolución tecnológica.

Hoy, ha surgido una nueva y poderosa competencia para las universidades motivado por la demanda creciente de educarse cada vez mejor, radicada en los sistemas de tele-enseñanza y autoeducación que, haciendo uso de las tecnologías modernas, va creciendo en forma paralela y, en algunos casos, más acelerada que las propias instituciones universitarias. No hay duda, Internet se ha convertido en la herramienta más eficaz que hoy existe para difundir conocimientos y la tecnología didáctica, en sí misma positiva, tiene un futuro formidable como complemento en la enseñanza.

Hay, pues, ante los escenarios actuales, unos aspectos de las universidades que deben mantenerse y otros que deben cambiar como consecuencia del doble reto de mantenerse a la vanguardia de la tecnología educativa y fortalecer los principios de rigor académico. Lo que debe preservarse son, esencialmente, sus valores, los principios éticos que norman su vida y definen su misión: la búsqueda de la verdad, el respeto a la diferencia, las formas rigurosas de aproximarse al conocimiento, etcétera. Al mismo tiempo hay que revalorar la función docente, plantear sin titubeos como se debe entender el trabajo de enseñar, formar y educar, de cara a la globalización, a la sociedad del conocimiento. Frente a ellas y con la revolución tecnológica de la información encima, hay universidades que se transforman para fortalecerse; universidades que no cambian y se van marginando; y universidades que surgen, algunas de las cuales se han autodenominado universidades virtuales.

Hoy se estima que el conocimiento se duplica cada cinco años. Economías que eran muy pequeñas hace algunos años y que hoy son realmente poderosas, corresponden a países que durante las últimas décadas tuvieron, entre otras, una constante: el incremento gradual y sostenido de su gasto en educación y en particular en educación superior e investigación científica. Existen en el mundo aproximadamente 7 mil universidades registradas; pero de los 560 millones de jóvenes que deberían acceder a ellas, sólo lo hacen 88 millones [bib09]. En los países con alto ingreso, uno de cada dos jóvenes tiene acceso a la universidad, mientras que en los países con bajo ingreso sólo llega uno de cada diez. Queda establecido que se tiene que dar un mayor impulso a las universidades dada su responsabilidad y que se tienen que hacer los cambios que le permitan enfrentar exitosamente las nuevas condiciones globales y nacionales en las que están inmersas.

1.2.1. UNAM

Parece necesario hacer un repaso de los antecedentes históricos específicos de la UNAM, y aunque parezca tema de otro trabajo, será útil este ejercicio para ubicarla en los cambios descritos y dar una visión del papel que juega en la sociedad. También es importante hacer notar el rol que tienen las instituciones contenidas y así comprender porque cada una presenta cierta independencia y debe ser tratada como un ente con mecanismos y necesidades propios.

Al final de la colonia, ocurre un acontecimiento importantísimo para la educación superior en México: se funda en 1772 el Real Seminario de Minas o Colegio de Minería y tras él otras instituciones de tendencia moderna en la educación y la cultura. En contraste, el proyecto educativo liberal pretendía, en lo que se refiere a educación básica, su extensión a capas amplias de la sociedad y su alejamiento de la enseñanza confesional; en lo que se refiere al nivel superior una enseñanza formadora de profesionales, científicos y hombres libres que atendieran las nuevas necesidades de la producción y los servicios y la demanda de una educación para el trabajo presentada por los sectores medios de la nueva sociedad [bib09].

En 1867 se crea, para el nivel básico, la enseñanza pública sostenida por el gobierno, obligatoria para todos los niños y niñas y laica (reforma de 1869). Para la enseñanza media se instituye la Escuela Nacional Preparatoria (ENP) y para la enseñanza superior una serie de escuelas nacionales de carácter profesional, entre otras la de ingenieros, la de medicina, la de jurisprudencia, la de agricultura y veterinaria y la normal para maestros, todas ellas relativamente independientes. Sin embargo, se notaba una ausencia: un centro de cultura superior en el cual se estudiaran las ciencias, las humanidades, se hiciera investigación y en el cual los jóvenes, que al terminar los estudios medios de la ENP optaran por prepararse en ese sentido, tuvieran una institución de educación superior donde hacerlo.

En la figura de Justo Sierra, se concretó un proyecto: Fundar una universidad integrada por las escuelas profesionales y las ya existentes. Tiempo después se fundó la Universidad Nacional de México.

Los dos puntos más relevantes, en cuanto a concepción y estructura académica de la nueva universidad, son el concepto de integración de un conjunto de escuelas profesionales como tales en una especie de federación (Escuela Nacional de Ingenieros, Escuela Nacional de Medicina, Escuela Nacional de Jurisprudencia) y la incorporación de la ENP. Tenemos pues, un sistema en el que cada escuela profesional continúa siendo una unidad con características propias y tendencia hacia la autosuficiencia. A lo largo del tiempo, se fueron incorporando a la Universidad diversas instituciones de investigación, algunas de las cuales existían desde el siglo XIX, como el Observatorio Astronómico Nacional o el Jardín Botánico.

Así se conforma la UNAM actual, con esto no queremos decir que la Universidad de hoy sea la misma que la de 1945 (fecha en que se aprobó su Ley Orgánica), significa que los elementos básicos de su estructura, con su significado y repercusión académica son los mismos. Un grupo de escuelas y facultades que, si bien se ven reunidas, no pierden su carácter de institución por sí mismas, y un conjunto de institutos con una tarea básica de investigación coordinados en dos subsistemas, uno de ciencias y otro de humanidades (y ciencias sociales).

Cada escuela o facultad conserva, cuando se la ve como institución por sí misma, un carácter de escuela profesional, estructurada internamente y orientada por la enseñanza de la o las profesiones correspondientes y con tendencia a la autosuficiencia en la realización de su tarea educativa. En el caso de los dos subsistemas de investigación, su estructura interna se puede decir que es departamental o sustentada en una organización

disciplinaria. Estas dos vías estructurales, la reunión de escuelas y facultades de tendencia profesional y los dos subsistemas de investigación de tendencia disciplinaria, se superponen, pero difícilmente podemos decir que se integran en un todo estructural. Por otro lado, la Escuela Nacional Preparatoria y el Colegio de Ciencias y Humanidades, continúan integradas como dos escuelas más a la estructura académica de la UNAM y su función sigue siendo propedéutica hacia los estudios profesionales. Las Escuelas Nacionales de Estudios Profesionales y las Facultades de Estudios Superiores, si bien se integran como tales al conjunto de escuelas y facultades, no se puede decir que representen a una profesión o rama profesional. En cada una de ellas se puede estudiar una decena de carreras distintas, aunque estructuralmente hablando, ocupan una posición similar. Además debemos considerar que en estas escuelas estudia 40% de los alumnos de licenciatura de la UNAM y que cada una de ellas ha evolucionado en su estructura interna de manera distinta

Desde 1945, naturalmente que ha habido enormes cambios, tanto en la expresión concreta de esa estructura, como en las situaciones sociales, objetivos académicos, relaciones con el sistema educativo en general y otras cuestiones que influencian o condicionan a la Universidad. En el terreno de lo cuantitativo las diferencias son tan grandes que en realidad configuran un cambio cualitativo. En 1945 la UNAM tenía unos cuantos miles de alumnos; hoy la cifra es del orden de 270 000; de ellos, aproximadamente 100 000 corresponden al nivel medio superior y 170 000 al superior. Otro aspecto de suma importancia es el posgrado, que hoy ocupa una posición relevante, mientras que en 1945 no la tenía. Hoy el subsistema de posgrado tiene unos 20 000 alumnos. El personal académico de hoy tiene una inscripción y relación con la UNAM totalmente distinta. En primer lugar hay aproximadamente 10 000 académicos de carrera y 17 000 profesores de asignatura. En 1945 casi todos eran de asignatura. De esos 10 000 académicos de carrera unos 1 300 corresponden al bachillerato, 3 300 a los subsistemas de investigación, 5 000 al sistema de escuelas y facultades y el resto a diversas dependencias de apoyo. Destacamos que 40% del personal de carrera asociado a la enseñanza superior está adscrito a los institutos y centros de investigación [bib09]. Adicionalmente, esto nos indica que los subsistemas de investigación, que antes podían verse como un agregado a una estructura académica sustentada en las escuelas profesionales, son, en la actualidad, una parte determinante de la UNAM.

Es notable, que la estructura basada en escuelas profesionales autosuficientes tiene su origen en la atención a la demanda social de profesionistas y esta a su vez surge de las necesidades de la producción y los servicios. Hoy pues, estamos en la llamada sociedad del conocimiento, caracterizada por la vertiginosa velocidad con que se acumula, se genera y se aplica el conocimiento y la tecnología. Es en los niveles básico, medio superior y superior del sector educativo donde el cómputo y las telecomunicaciones han cosechado grandes frutos, pues han enriquecido toda la enseñanza por su capacidad de comunicar, almacenar y procesar información, manejar números en cálculos y simulaciones y apoyar la educación formal, continua y a distancia. En la enseñanza superior, son medios fundamentales para aumentar la productividad y elevar la calidad de un sinnúmero de actividades.

Hoy en día, no se concibe el trabajo universitario sin el uso del correo electrónico, foros de discusión, enormes acervos bibliográficos, bancos de datos, videoconferencias, páginas web y herramientas de oficina como el procesador de texto, la hoja de cálculo, las presentaciones, la construcción de modelos en supercomputadoras y mucho más.

Desde 1958 la UNAM ha logrado un gran progreso en todas sus tareas al adoptar las tecnologías de la información, comenzando con la instalación de la primer computadora en América Latina. Internet y las telecomunicaciones vía satélite permiten la integración institucional que acerca a las entidades universitarias dispersas en el territorio nacional, en Estados Unidos y Canadá. También permiten el acercamiento con estudiantes, maestros e investigadores de otras casas de estudios y el acceso a acervos y complejos instrumentos no disponibles de otro modo en la UNAM. En la UNAM, el uso de las tecnologías de la información desempeña ya un papel fundamental en el propio desarrollo de la institución, pues gracias a ellas se han generado las condiciones idóneas para mejorar la calidad de la enseñanza y aumentar la producción académica. En la actualidad, los servicios de Internet y las telecomunicaciones han transformado favorablemente las condiciones de acceso al conocimiento y la difusión del mismo en nuestra casa de estudios. Además del acceso a la información desde lugares lejanos y la copia de archivos entre computadoras, el uso de Internet permite una comunicación interpersonal basada en el correo electrónico y otros sistemas de recepción y envío de mensajes en línea. Estas valiosas herramientas para la comunicación por computadora han permitido a la UNAM desarrollarse en una forma inimaginable desde hace un par de

décadas. Por ello, desde 1958 ha habido una "expansión continua" del cómputo en la UNAM. Como sería difícil historiarla, sólo se mencionarán las etapas más importantes de ese proceso:

1958. Centro de Cálculo Electrónico (CCE). El cómputo en la UNAM tiene su origen el 8 de junio de 1958, con el establecimiento del Centro de Cálculo Electrónico, cuyo actor principal fue la computadora IBM-650. Tenía el propósito de realizar investigaciones en matemáticas, física y actuaría, e inició su funcionamiento con los departamentos de Cibernética y Teoría de la Información, Teoría Matemática de la Programación y Servicio de Cálculo.

1965. Se inició la actividad administrativa del cómputo al instalarse una IBM-1440. Se crea el Departamento de Sistemas de Patronato, la Sección de Máquinas de Servicios Escolares y posteriormente, como resultado de la fusión de ambos, se formaría la Dirección General de Sistematización de Datos.

1970. Centro de Investigación en Matemáticas Aplicadas, Sistemas y Servicios (CIMASS). Con la intención de integrar en una sola dependencia el apoyo del cómputo para la Universidad en lo académico y administrativo, en 1970 se fusionaron el Centro de Cálculo Electrónico y la Dirección General de Sistematización de Datos, para crear, el 10 de diciembre de ese mismo año, el Centro de Investigación en Matemáticas Aplicadas, Sistemas y Servicios. Entre otros proyectos, se llevó a cabo el Sistema de Control Escolar, el Sistema para Cálculo de Estadísticas, el Sistema de Recuperación de Información, el Catálogo y Diagnóstico de Enfermedades y el Cálculo de Estructuras en Ingeniería.

1973. Centro de Servicios de Cómputo (CSC) y Centro de Investigación en Matemáticas Aplicadas y Sistemas (CIMAS). Creados con el fin de propiciar el desarrollo independiente de la investigación y los servicios informáticos, motivados a partir de la reorganización del CIMASS.

1981. Programa Universitario de Cómputo (PUC). El 15 de octubre de 1981, se creó el Programa Universitario de Cómputo, que reestructuró los Centros de Servicio de Cómputo desde una nueva perspectiva: la de brindar servicio especializado, y centralizado, a las áreas de docencia, investigación, administración académica y administración central.

1985. Consejo Asesor en Cómputo (CAC), Dirección General de Servicios de Cómputo Académico (DGSCA) y Dirección General de Servicios de Cómputo Administrativo (DGSCA). Con el objetivo de contar con un plan estratégico de desarrollo del cómputo institucional, una coordinación más efectiva y una instancia promotora, el 14 de mayo de 1985 se estableció el Consejo Asesor en Cómputo como un cuerpo colegiado formado por funcionarios y académicos destacados en el área. Simultáneamente, se crearon la Dirección General de Servicios de Cómputo Académico, que daría servicio a la docencia, la investigación y la administración académica, y la Dirección General de Servicios de Computo Administrativo, que auxiliaría a la administración central.

1986. Inicio del servicio de correo electrónico.

1989. F.o. en México. Primeros enlaces de fibra óptica en México. Primeros nodos Ethernet y Token Ring de la Red Universitaria de Cómputo. Integración de las primeras redes locales. Enlace satelital con Cuernavaca, Ensenada y con la NFS Network. Incorporación de universidades de provincia a la red universitaria.

1990. Programa de reestructuración de telecomunicaciones. Primeros 25 centros de cómputo integrados a la red. Inicio de Internet en México.

1991. Primeras comunicaciones telefónicas digitales vía satélite. Ampliación de la red a 50 centros y 700 computadoras. La UNAM instala la primer Supercomputadora en Latinoamérica, la CRAY YMP/432. Se implementan: Telnet, FTP, y listas de correo.

1995. Implementación de servicios de videoconferencia.

1.2.2. Dirección General de Servicios de Cómputo Académico

Actualmente, la Dirección General de Servicios de Cómputo Académico está integrada por las direcciones de Telecomunicaciones , de Cómputo para la Investigación, de Cómputo para la Administración y de Cómputo para la Docencia. Su tarea fundamental es lograr que la Universidad disponga de los instrumentos informáticos idóneos para cumplir lo mejor posible sus actividades.

Cabe destacar que cada entidad universitaria cuenta hoy con su propia área de cómputo, donde se realizan las actividades cotidianas que le corresponden conforme a un esquema totalmente descentralizado. La función de la DGSCA consiste en apoyarlas, brindarles servicios de primera línea, en especial Internet, y poner a su alcance los avances tecnológicos.

Desde 1990, al crearse la Dirección de Telecomunicaciones, la UNAM se convirtió en una de las primeras instituciones del mundo que integró los servicios de telefonía a la red digital de datos, lo que le permitió emprender programas de gran envergadura. Recordemos que entonces se contaba con un conmutador telefónico con poco más de 2 000 extensiones y unos cuantos cientos de computadoras en red. Hoy, la UNAM cuenta con 15 000 teléfonos directos y más de 30 000 computadoras con servicio de Internet que prácticamente unen a todos los edificios y cámpus de la casa de estudios. En esta década, el desarrollo informático de la UNAM se concibió como el detonador tecnológico del mejoramiento académico institucional. Resulta evidente el valor estratégico que la Universidad asigna a las nuevas tecnologías de la información. Podríamos incluso decir que en la actualidad se han convertido en el hilo conductor al futuro de nuestra institución.

La Dirección de Telecomunicaciones, tiene como tarea garantizar los enlaces locales, regionales, nacionales e internacionales, para que los usuarios estén en la posibilidad de mantener comunicación. La infraestructura de telecomunicaciones de la Universidad comprende la Red Universitaria de Cómputo (RedUnam) y el Sistema Telefónico Digital que, mediante la integración de los diferentes servicios y recursos del cómputo y las telecomunicaciones, elimina la barrera de las distancias. En 1989, la UNAM introdujo Internet en México, con la meta de que todas las áreas de la institución y todos los centros de enseñanza superior nacionales contaran con ese importante servicio. En 1995, se inició el servicio de videoconferencias interactivas y luego, a partir de él, se creó la Red Nacional de Videoconferencias, que hoy reune cerca de 200 salas localizadas en 40 instituciones educativas nacionales.

Pensando que el trabajo y el saber universitario deben ponerse al servicio de todos, se tienen que establecer los mecanismos que permitan a profesores, investigadores, técnicos y estudiantes preservar sus contenidos académicos adecuadamente, difundirlos con amplitud y convertirlos en insumo para la generación de nuevos conocimientos y la formación de recursos humanos. Para ampliar la calidad y la cobertura de la educación superior resulta impostergable lograr que la mayoría de las entidades académicas integren las nuevas tecnologías de la información a su actividad educativa.

1.3. Redes de alto desempeño

El diseño de redes es complejo: parte ciencia, parte arte. En varios aspectos es similar con otras formas de diseño, en el sentido en que se establecen los requisitos, se encuentran los componentes substanciales, se acoplan, se estructura, se prueba y se libera para su uso. Sin embargo, existen otros factores en el diseño de redes. Para empezar, no es fácil lograr articular los requisitos de una red, aún cuando se trate de proporcionar servicio a una docena de usuarios. Se requiere de ciertos conocimientos para trasladar las necesidades de un grupo de personas al diseño real (entendiéndose por real la seguridad, funcionalidad, flexibilidad y bajo costo). Posteriormente, cuando la red se encuentra instalada y funcionando, es parte medular de la infraestructura de una institución por lo que se vuelve crítico su funcionamiento. Por otro lado, la importancia de la administración y el mantenimiento recae en la complejidad de las redes modernas —y las grandes expectativas que se forman alrededor. Teóricamente, es posible proporcionar a un usuario acceso rápido y sin problemas a la información, en el momento que quiera, independiente del lugar y en una variedad de configuraciones. En la práctica, se requiere de mucho trabajo para lograr algo similar a lo que se desea. Aún cuando el diseño sea satisfactorio, existen partes de la tecnología que, dada su complejidad, deben ser

estudiadas por separado antes de utilizarlas en forma colectiva. Finalmente, cuando estos componentes tan complejos son interconectados, no es 100% predecible el desempeño que se obtendrá pues ejemplos bastan para encontrar redes que proveen ventajas a sus usuarios y otras que han resultado ineficaces y en desuso.

Para obtener una red de alto desempeño, se deben conocer los principios que rigen a las redes y su diseño, pues nos ayudaran a mantenernos en contacto con la tecnología y sus avances sin importar cuantos y que tan rápidos sean. Es necesario tener una visión clara de lo que realmente significa el término "red de alto desempeño" y sus beneficios. Podemos tomar la siguiente definición: "Una red de alto desempeño es un recurso que permite la transferencia y el procesamiento de información a través de toda la gama de operaciones de una organización. Debe proveer a cualquier usuario en la red con los servicios que necesita, indistinto de la localización física de dichos servicios" [bib02].

Existen algunos aspectos de nuestra definición que deben ser remarcados:
- La red debe presentarse para los usuarios y administradores como un único y homogéneo recurso —sin importar la gran variedad de tecnologías con las cuales puede estar compuesto.
- La red debe ser configurada para soportar directamente los procedimientos, procesos y operaciones —el usuario debe estar concentrado en realizar su trabajo en lugar de lidiar con la red.
- La red debe tener definidos estándares de administración, mismos que deben abarcar diferentes niveles de rendimiento, disponibilidad y confiabilidad.

No tiene mucho sentido tener una red de alto rendimiento si no se maximizan las ventajas que ésta puede ofrecer. Así que es importante preguntarse, ¿qué se hace con una red de este tipo?, ¿para qué sirve? y ¿qué beneficios se obtienen al invertir en una?.

Esto se logra teniendo una visión clara de los siguientes aspectos:
- Requisitos del usuario (aplicaciones, tráfico, rendimiento, ancho de banda, velocidad de transmisión, etc.)
- Necesidades (costo, redundancia, capacidad de crecimiento, adaptabilidad, etc.)
- Integración (métodos para relacionar al usuario con la red)

Queda claro que no se puede salir a la calle y adquirir un kit de red previamente ensamblado y tratar de implantarlo en la infraestructura existente, por el contrario, todas las partes involucradas tienen que realizar un gran esfuerzo para obtener una red verdaderamente efectiva. En el contexto de la UNAM, existen dos entidades principales:

- *Usuario.* Una red es instalada por un grupo de personas para beneficio de otro grupo de personas. Cada grupo tiene un cúmulo de necesidades que ayudan a medir en forma porcentual el éxito de una instalación. En conjunto, los grupos forman una comunidad que debe recibir ciertos beneficios de la red. Es importante considerar quienes son las personas involucradas en el diseño, su papel, sus responsabilidades y sus necesidades, por ejemplo: el director, los usuarios, los administradores, los proveedores y la normatividad.

- *Instituciones educativas.* Las instituciones educativas modernas necesitan trabajar cada vez más rápido, mejor y eficiente para mantenerse competitivas. El papel, fax y teléfono ya no son suficientes y existe una clara necesidad de sistemas de comunicaciones y computadoras que permitan a las personas relacionarse entre sí independiente de su ubicación geográfica. Es decir, proveer una infraestructura de información flexible y uniforme que permita olvidarse de la distancia, satisfaga los requisitos y se readapte a las necesidades futuras.

1.3.1. Red tradicional vs. Red de alto desempeño

En su forma más simple, una red no es más que un grupo de entidades interconectadas. Su función es permitir el flujo de servicios de voz, datos y video para que los usuarios finales puedan acceder, procesar, enviar y almacenar la información con la que trabajan. En el caso de una red de alto desempeño, ésta se conforma de tantas partes diferentes que un solo proveedor no puede proporcionar una solución efectiva a cada requisito del usuario.

Las redes que permiten un funcionamiento a gran escala requieren más que una simple representación (figura 1), por lo que existen algunas observaciones:

- *Administración*

Primero, una red de alto desempeño no es una entidad estática —presenta cambios continuos. Y algunos de esos cambios son intencionales; por ejemplo, nuevos sitios, nuevos servicios en línea y nuevas configuraciones en routers para mejorar la velocidad y el acceso. Existe otro tipo de cambios (menos deseables) como fallas de equipos, variaciones en el suministro de energía eléctrica, pérdida de información que afecte al cómputo y las comunicaciones, etc. Para que una red ofrezca un soporte adecuado, debe ser manejada como un solo recurso y administrada para satisfacer las necesidades de los usuarios.

- *Complejidad*

El segundo punto es que la representación tiene varios puntos de vista. Así como se tienen conexiones físicas y lógicas entre los sitios, también se necesitan aplicaciones compatibles, un formato de datos común, nombres y direcciones homologados, etc., y cada parte es vital para una operación satisfactoria. Para trabajar con cualquier fuente de información, es necesario integrar una variedad de protocolos, aplicaciones y medios de conexión para evitar incompatibilidades y fallas en el procesamiento de información.

- *Seguridad*

El punto final es que los recursos importantes deben ser protegidos. Cualquier red está expuesta al abuso de cualquiera en cualquier lugar. Al manejar información valiosa, la seguridad —física y lógica— es relevante. El nivel de seguridad debe estar balanceado con la flexibilidad y facilidad de uso vista por el usuario.

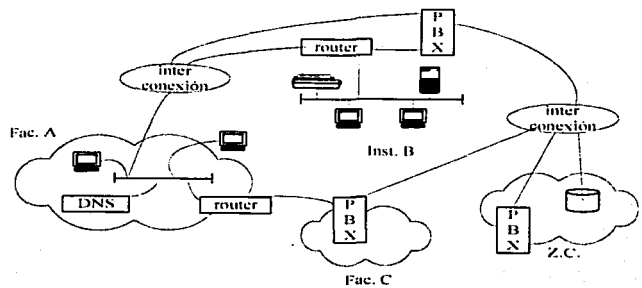


Figura 1. Representación de una red a gran escala

La red ilustrada en la figura 1 contiene varios componentes de distintos proveedores, inclusive en distintas versiones, tales como:

- Redes locales, gateways, bridges, routers, multiplexores, etc.
- Conmutadores, teléfonos, enlaces dedicados, etc.
- Computadoras, software, controladores, terminales, etc.

Los distintos elementos han evolucionado con los años y merecen ser historiados desde dos puntos de vista: telecomunicaciones y computo. Cada uno tiene sus características, dinámica y forma de hacer las cosas, pero ambos tienen un rol significativo y contribuyen en las redes de alto desempeño.

1.3.2. Telecomunicaciones

Literalmente, comunicaciones a distancia. En la actualidad significa la transmisión no solo de palabras, también de sonidos, imágenes o datos en la forma de señales eléctricas o impulsos. Durante los últimos 100 años, el teléfono ha sido reconocido como la representación más familiar de las telecomunicaciones.

Recientemente, la telefonía se ha implementado en computadoras permitiendo que muchas personas, a través del Internet y el WWW, intercambien enormes cantidades de información.

Actualmente tan solo con apretar unos cuantos botones podemos hablar con familiares, amigos y de negocios alrededor del mundo. Es claro que la red telefónica ha sufrido un constante refinamiento en los últimos 100 años, ejemplo es que la telefonía moderna puede ser vista como una máquina distribuida globalmente que opera como un solo recurso y es la red empleada por mucha gente para transferir voz y datos en forma de imágenes, texto y video.

Existen varias configuraciones para transferir información entre emisor y receptor y la opción seleccionada refleja el tipo de comunicación que se requiere. Por ejemplo, los humanos somos tolerantes, dentro de límites aceptables, al ruido y los errores de transmisión cuando nos comunicamos, pero las computadoras tienen la característica opuesta. Por esto se presentan los principales conceptos manejados en las telecomunicaciones.

- *Redes analógicas y digitales*
  - Las primeras telecomunicaciones fueron analógicas; utilizaban señales continuas para transmitir información. Las redes analógicas de voz de los 70's han migrado, parte por parte, a la par de las redes digitales de hoy día. Esto comenzó con las conexiones de larga distancia e intercambio y, más recientemente, se ha extendido a las redes locales.
  - Las comunicaciones por computadora, basadas en señales digitales discretas, pueden usar conexiones analógicas pero están limitadas. La capacidad de las redes digitales ha crecido bastante rápido y es posible trabajar con servicios de voz, datos, texto e imágenes.

- *Conmutación de circuitos y conmutación de paquetes*
  - La característica principal de la conmutación de circuitos es que una conexión punto a punto es realizada entre los dos extremos, y se mantiene hasta que la comunicación termina. La red de telefonía pública es un claro ejemplo.
  - Por otra parte, la comunicación entre computadoras o dispositivos terminales se lleva a cabo en bloques en lugar de un flujo continuo. La conmutación de paquetes tiene la ventaja de que se pueden transferir los bloques sin necesidad de establecer una conexión directa entre los extremos, en su lugar, se utiliza una serie de enlaces concatenados en los cuales se almacena la información y se enruta al siguiente enlace. Para el enrutamiento se toman en cuenta las direcciones origen y destino, mismas que están incluidas en la cabecera de cada bloque. El termino paquete se refiere a la cabecera más la información. Internet basa su funcionamiento en la tecnología de paquetes y por su tamaño puede ofrecer varios caminos alternativos que representan la mejor opción acorde a cualquier necesidad.

- *Tráfico y bloqueo*
  - En una red con conmutación de paquetes, éstos compiten dinámicamente por los recursos (almacenamiento, procesamiento, capacidad de transmisión, etc.) aunque la red no conozca que tipo y cantidad de recursos se necesita para cada uno. Existe la posibilidad de que un equipo de comunicaciones acepte un paquete sin contar con los recursos requeridos, y en tal caso, estar admitiendo más tráfico del que puede procesar, llevando a una degradación en el servicio. Se necesita un control para asegurar que dicho tráfico no sea constante o, en caso de suceder, exista una recuperación satisfactoria.
  - En una red con conmutación de circuitos, la competencia por los recursos se lleva a cabo a través del bloqueo. Esto quiere decir, que la llamada de un usuario evita que otro tenga acceso al mismo enlace, pues el circuito se encuentra reservado —independiente del uso— hasta que la comunicación concluya. Generalmente, las redes con conmutación de circuitos son diseñadas para balancear la cantidad de equipo instalado con el número de usuarios en la red.

- *Rendimiento*
  - En una red conmutada en circuitos, como la telefonía pública, se proporcionan las conexiones bajo demanda, ofreciendo los recursos necesarios. El retraso en la conexión es pequeño, constante y la calidad del servicio no puede ser controlada por el usuario.

- En una red conmutada en paquetes, existen colas de espera en cada equipo de comunicaciones. Por lo que el retraso es variable dependiendo de la cantidad de tráfico encontrado en el direccionamiento.

Internet ha crecido aceleradamente durante los últimos 25 años y enlaza a millones de personas alrededor del mundo, muchas de las cuales emplean la telefonía pública para conectarse. Las compañías telefónicas tradicionales han tenido que evolucionar para continuar siendo competitivas, ya que hoy es mayor el número de proveedores dentro de las comunicaciones de voz y datos. En los últimos años han surgido las alianzas entre compañías que buscan expander sus horizontes de cobertura y así poder ofrecer servicios como redes privadas virtuales. Cabe mencionar que las redes privadas virtuales son sumamente atractivas desde el punto de vista del usuario porque le parece transparente el estar conectado a través de muchos nodos dejando la complejidad y los problemas potenciales a los operadores de las compañías de telecomunicaciones, finalmente encargados de la nube de interconexión. De cualquier forma hay que tener en cuenta que este tipo de servicios, aunque con muchas ventajas, no son la panacea.

Ha sido un crecimiento enorme para el área de las telecomunicaciones y no se puede dar por concluido su avance ni tampoco que lo que se ha desarrollado funcionará a la perfección. Muchas de las aplicaciones que operan en las diferentes redes han surgido de la industria del cómputo y, como se había mencionado, entre ellas existen diferentes formas de hacer las cosas.

1.3.3. Cómputo

La adopción de las computadoras personales y las redes locales durante los 80's ha permitido el intercambio de información entre grupos de computadoras y sus usuarios. Actualmente es de lo más natural tener acceso a información de una base de datos distante, descargar aplicaciones de un servidor, enviar mensajes a personas de diferentes paises y compartir archivos con compañeros de trabajo, y todo desde la computadora.

Las redes que permiten este tipo de servicios son entidades sofisticadas y complejas. Confían su desempeño a varios componentes relacionados, que deben su existencia al trabajo esforzado y conjunto de muchas personas durante muchos años.

En los 70's, las computadoras eran máquinas caras y frágiles que tenían que ser resguardadas por especialistas y ubicadas en ambientes controlados. Podían ser utilizadas para conectar directamente una terminal o usar una línea telefónica y un módem para obtener acceso de manera remota. Debido a su costo, tendían a ser recursos centralizados en los cuales los usuarios tenían que tramitar cualquier tipo de acceso. Durante esta era, las redes de computadoras no eran comercialmente viables, sin embargo se hicieron desarrollos significativos para distribuir los recursos de cómputo y dar origen a lo que ahora se conoce como Internet.

Uno de los eventos más dramáticos en lo que a cómputo se refiere ha sido la introducción y el rápido crecimiento de las redes de área local (LAN). En su nivel más simple, una LAN no es más que un medio de transmisión compartido con reglas que rigen el acceso. El tipo de LAN más difundido, Ethernet, emplea un mecanismo en el cual cada dispositivo solamente puede utilizar el medio una vez que ha sido comprobado que ningún otro se encuentra transmitiendo, considerando algoritmos para solucionar el caso contrario. Otro tipo de LAN bastante popular, FDDI, cumple el mismo objetivo pasando una señal que indica el momento en que puede comenzar a transmitir cada uno de los usuarios conectados al anillo.

Ethernet y FDDI son ejemplos de redes LAN y existen otros tipos de arquitecturas, pero, a pesar de las diferencias, todas comparten una caracteristica: su rango es limitado aunque son lo suficientemente rápidas para los dispositivos conectados a ellas.

Además de facilitar la compartición de recursos, las LAN modernas ofrecen una variedad de sofisticados servicios, que van desde paquetes de administración de redes que permiten establecer políticas de uso hasta servidores que permiten el acceso a sus clientes, pasando por administradores de impresión, bases de datos, correo, etc.

Para poder convivir con otras redes y, en determinadas circunstancias, ofrecer más servicios a un mayor número de usuarios, los bridges y routers son utilizados. Los bridges con la capacidad de conectar redes del mismo tipo, y los routers con la capacidad de trabajar con diferentes tipos de redes conectadas a sus puertos. La configuración física para lograr tal expansión está dictada, mayormente, por el costo, por lo que hay que evaluar el rango de opciones y seleccionar la que presente el mejor costo-beneficio.

A pesar de que en los 80's no todas las computadoras que salían al mercado eran compatibles, hoy día se ha logrado un nivel de estandarización que les permite intercomunicarse de forma efectiva, logrado principalmente por los siguientes factores:

- *Cliente-servidor*
  El cliente (usuario en PC) requiere un servicio (imprimir) y el servidor (estación de trabajo conectada a la LAN) lo ofrece. Esta visión indica que existe una separación de lo que anteriormente era centralizado.

- *Tecnología de objetos*
  Surge de la premisa de que los sistemas de cómputo deben ser construidos de partes perfectamente definidas —objetos que son desarrollados e implementados para que puedan ser tratados como agentes independientes. Esto permite la modularidad de las partes.

- *Sistemas abiertos*
  Abarca la concepción de construir sistemas de cómputo que puedan ser rápidamente interconectados y en consecuencia distribuidos. Es decir, permitir a una persona comprar computadoras de distintos proveedores, instalarlas de la forma más conveniente, emplear cualquier medio para enlazarlas y operarlas de tal manera que se pueda obtener lo mejor de cada componente.

- *Seguridad*
  Con un mayor número de computadoras conectadas a Internet, y aún en redes locales, cada vez se vuelve más importante la seguridad. A partir de 1970 se han creado estándares y métodos de encripción para el intercambio de información y evitar que ésta se comprometa al ser interceptada por terceras personas.

- *Administración*
  A pesar de que los conceptos esenciales y los métodos para la administración de una red han recibido mucha atención en los últimos años, no existe todavía una integración completa de las distintas herramientas creadas para lograr que las redes de computadoras sean efectivamente supervisadas. Se necesita mucho trabajo y esto compromete el balance entre la administración y calidad en el servicio.

El reto para el diseñador de redes consiste en la integración de estos componentes en forma coherente con un costo asequible. El conjunto de componentes no solamente debe interactuar, también debe ser operado y administrado individualmente. Para lograr este avance, es necesario ir más allá de dibujar cuadros con líneas entre ellos, ahora se requiere mostrar la capacidad de los enlaces, de los equipos, protocolos, etc.

1.3.4. Diseñador

Existen muchos retos para el trabajo del diseñador, y su efectividad puede ser medida de acuerdo al siguiente criterio:

- *Necesidades.* Proporcionar las facilidades para que las actividades se realicen más rápido, mejor y más fácil, entendiéndose que la red debe soportar las aplicaciones para las cuales fue diseñada.

- *Costo.* Contemplar no solo el costo de adquirirla e instalarla, también el costo de mantenerla.

- *Rendimiento.* El diseño debe permitir que las transacciones se ejecuten lo suficientemente rápido para que el usuario esté satisfecho y mantener las prestaciones durante los picos de tráfico.

- *Confiabilidad.* Significa que los elementos que contribuyen en una sesión trabajen correctamente al mismo tiempo. Un buen diseño tiene tolerancia a la caída de uno o varios elementos sin que afecte al usuario.

- *Disponibilidad.* Cierto nivel de mantenimiento y administración es inevitable en cualquier red. La manera en que esto afecta al usuario es algo relativo.

- *Adaptabilidad.* Diseñar para el cambio es un factor importante en áreas en las que constantemente hay cambios de estructura, procedimientos y forma de trabajo. Un buen diseño debe acomodar nuevos servicios sin que afecte su funcionamiento.

- *Administrabilidad.* Una red debe ser diseñada de tal forma que pueda ser administrada, así que cada elemento debe ser compatible con los sistemas de monitoreo y administración existentes en el mercado.

El Internet crece y mejora constantemente, lo que representa un reto para todos aquellos que quieran mantenerse actualizados en cuanto a toda la tecnología involucrada. Sin duda, los motivos originales por los cuales fue creado el Internet se han mantenido, exceptuando aquellos factores que ponen en riesgo la sana convivencia entre la comunidad.

Para la UNAM, el Internet se ha convertido en una herramienta sumamente importante para llevar a cabo las actividades sustantivas que la rigen, como son la docencia, la investigación y la difusión de la cultura, pero es necesario encontrar el balance adecuado entre todo el poder tecnológico existente y las características específicas de la UNAM, como la capacidad de asimilación de dichos avances, la difusión de la tecnología, la investigación al respecto, los cambios tan frecuentes motivados por su propia naturaleza, etc. De esta forma, podemos comprender porque el énfasis en convertir las redes existentes en algo mas que cables y aparatos electrónicos, que en muchas ocasiones representan un gasto muy alto para los beneficios que se obtienen, llegando, en algunos casos, a ser un obstáculo para las funciones vitales.

Capítulo 2. Metodología para el diseño

2. 1. Teoría básica para el diseño de redes

La tarea de realizar un diseño para soportar las diversas operaciones trae consigo que éste comience desde cero. Dado que no hay una base sobre la cual trabajar, se tiene la libertad para construir lo más adecuado.

El primer punto a remarcar, es que aún cuando se conozca la red actual, en caso de que no se pueda comenzar desde cero, existirán puntos de conexión a considerar, sistemas externos a conectar, fuentes o bases de datos a acceder y procesos esenciales que deben ser soportados. Así que lo primero es establecer la estructura del área en la cual se va a trabajar. Esto junto con el resultado final que el usuario espera obtener, constituyen la información vital para construir un conjunto completo de requerimientos de red. Este es el primero de una serie de pasos sistemáticos que deben ser completados por el diseñador, estableciendo el punto de partida y el objetivo final.

El segundo punto que debe ser subrayado acerca del diseño de redes es que éste no es prescriptivo. Debe ser elaborado sistemáticamente para que las ideas y soluciones evolucionen con los requerimientos. Al considerar la necesidad de analizar las soluciones, se puede dar un primer bosquejo de las principales etapas del diseño [bib04].

La UNAM agrupa casi todas las variantes de redes LAN y LsLAN existentes, que van desde el uso de repetidores hasta routers, de coaxial grueso hasta fibra óptica, etc. Esto tiene su origen en varios factores incluyendo el acceso libre y sin restricciones a los documentos relacionados a la evolución tecnológica, las facilidades para llevar a cabo la investigación sobre nuevos productos y aplicaciones y la colaboración para crear e impulsar la tecnología. De igual forma, la UNAM reune entidades con características propias y tendencia hacia la autosuficiencia.

En este sentido, es claro que cada dependencia tiene necesidades que deben ser satisfechas de manera única, empleando todas aquellas herramientas que le permitan desarrollarse eficientemente. Para lograrlo, primero se debe conocer el entorno de trabajo en la UNAM en lo que se refiere a cómputo y telecomunicaciones, para así poder crear una metodología que pueda ser la base sobre la cual se planteen nuevos proyectos y soluciones y se maneje la infraestructura existente.

Los puntos previos a considerar abarcan el aspecto social y tecnológico, lo que representa un doble trabajo para el diseñador. Por un lado, cumplir con las espectativas que se plantea el mismo usuario, quizá por su poco o vasto conocimiento, y por otro lado, lidiar con la tecnología pues muchas veces la teoría no concuerda con la realidad, por lo que los resultados obtenidos no siempre son los esperados, aun cuando se sigan al pie de la letra las recomendaciones al respecto.

En el ámbito de la UNAM, la situación es la siguiente:

- Las personas que tienen actividades en la UNAM abarcan casi todas las áreas del conocimiento. Esto trae como consecuencia un sinnúmero de aplicaciones que sería difícil enumerar.

- Generalmente, cada entidad cuenta con un responsable en lo que a cómputo y telecomunicaciones se refiere, sin embargo, no todos tienen el mismo nivel de aprendizaje y experiencia.
  - Al tener usuarios con pocos antecedentes, la ventaja es que la DGSCA, como la entidad designada para apoyar cualquier proyecto relacionado, puede mantener el control sobre las ampliaciones y/o modificaciones que se den en la red de cómputo de la UNAM; la desventaja es que absorben mucho tiempo del diseñador e imposibilita su trabajo hacia actividades de mayor importancia o emergencia.
  - Los usuarios con un buen nivel de experiencia liberan al diseñador de cierta carga de trabajo ya que tienen los antecedentes necesarios para tomar la iniciativa en la elaboración de proyectos y solución de fallas en la red que administran. Por otro lado, se corre el riesgo de que implanten redes que

impacten severamente el rendimiento de la red de backbone de la UNAM, al no conocer la topología y consideraciones externas a la red local.

- En la mayoría de las ocasiones, se presuponen las necesidades en la etapa de diseño. Es muy importante recalcar la relevancia que tiene el recabar los requerimientos con el mayor detalle posible. Muchos son los casos en los que el usuario ocupa su área de trabajo y no encuentra servicios instalados, encuentra servicios de más o simplemente la aplicación exige demasiados recursos que no pueden ser satisfechos.

- Dada la apertura hacia nuevas tecnologías, se presenta el reto de dar soporte a los equipos y aplicaciones emergentes sin afectar los actuales. Esto va de la mano con diseños propios que no se dan a conocer sino hasta el momento en que impactan a otras áreas y/o dependencias.

- Un aspecto sumamente importante es que el proyecto original de RedUnam no pudo dimensionar la expansión tan acelerada que tendría; cualquier porcentaje de crecimiento ha sido sobrepasado. En gran medida, las nuevas redes, ampliaciones y la consecuente adquisición de equipo no han tenido una adecuada planeación, y a pesar de que en su momento solucionan las necesidades, a la larga resultan difíciles de administrar, incompatibles o insuficientes. Más aún, si se califica el rendimiento, éste no es el más deseable.

- La UNAM presenta una constante transformación motivada, en parte, por los nuevos retos que se le plantean como institución educativa en un entorno cada vez más competitivo. Esto acarrea cambios frecuentes en su infraestructura de telecomunicaciones. Áreas que actualmente se dedican a labores administrativas, pueden convertirse en espacios de investigación en un periodo de tiempo bastante corto, áreas que funcionan como bodega pueden convertirse en aulas de videoconferencia, etc. Bajo estas condiciones, el diseño debe ser a futuro, mas que satisfacer solamente los requerimientos del momento.

- Como sucede con la mayoría de los productos relacionados a la tecnología, siempre habrá innovaciones y cambios, los cuales deben ser adecuadamente manejados y tomar lo que más convenga. El enfoque principal es en las redes LAN y LsLAN en lugar de la red backbone de la UNAM, ya que, aunque es probable que necesite soluciones más robustas, del cuidado que se tenga al diseñar las redes locales dependerá el rendimiento general de RedUnam. Muchas redes siguen basando su funcionamiento en repetidores, lo cual afecta severamente.

- El factor económico tiene su porcentaje de importancia, como en cualquier lugar. Las propuestas deben estar balanceadas entre el costo implicado para su adquisición y los beneficios ofrecidos, partiendo de lo expuesto en los puntos anteriores.

Esto debe servir para que el diseñador tenga una idea clara del punto de partida y las principales necesidades para las cuales debe elaborar propuestas que se puedan aplicar independiente de la entidad que se trate.

2.2. Metodología

Con un proyecto de la escala de muchas de las redes de alto desempeño de hoy en día, el trabajo de diseño puede ser extenuante. Con tareas tan complicadas, dividir las actividades puede ser la solución. La labor de diseño puede ser dividida en las siguientes áreas de trabajo:

- Captura de los requisitos y análisis.
- Diseño de la arquitectura.
- Diseño físico (equipo activo).
- Diseño del backbone.
- Diseño lógico (configuración).
- Diseño para la administración.
- Verificación y validación.
- Operación y evolución.

Captura de los requisitos y análisis

Usualmente, la primer tarea del diseñador es recabar y documentar los requisitos para establecer el punto de partida y hacia donde se quiere llegar. Dichos documentos frecuentemente constan de cientos de páginas, y un amplio tiempo debe ser dado para estudiarlos. Es buena idea remarcar los requisitos de mayor relevancia, así como preparar un escrito conciso que resuma las principales características e imperativos.

Durante este estudio, el diseñador está obligado a descubrir áreas en donde los requerimientos no provean suficiente detalle. El diseñador debe producir una bitácora con estas inquietudes. De ser posible, habrá que ir con la comunidad de usuarios para buscar mayor detalle de los requerimientos o con el canal formal previamente establecido para responder las inquietudes escritas. Las necesidades de red expresadas por el usuario son bastante específicas dado que tiene procedimientos de operación sumamente rígidos que necesita mantener. La presentación inicial de la red existente en la organización puede tener limitaciones claramente notorias, de igual forma la disparidad entre lo que existe y lo que se necesita puede estar enmarcado principalmente por limitaciones operacionales. Estas carencias son reflejadas en los requerimientos, los cuales ayudan a establecer los criterios para la nueva red. Ejemplos podrían ser:

- Interconectar completamente los sitios con los que se cuenta.
- Acceder la base principal desde los sitios remotos como parte esencial para las operaciones diarias.
- Descargar todos los archivos importantes cada noche para su almacenamiento.
- Garantizar tiempos de entrega para ciertas transacciones.
- Establecer la seguridad necesaria para un número pequeño pero importante de transacciones.
- Llevar a cabo cambios mínimos en las LAN actuales.
- Administrar y configurar la red fuera de las oficinas por un grupo de especialistas.
- Proveer una infraestructura que soporte el sistema de correo.
- Permitir la adición de nuevos sitios.

Estas necesidades deben ser redefinidas conforme se trabaja en el diseño. Aún este diseño a pequeña escala puede tomar tiempo considerable para ser analizado en su totalidad. Tomando esto en cuenta, vale la pena construir algunos escenarios de la red. Esto provee objetivos contra los cuales el diseño puede ser checado, al contrario de explorar todas las posibles opciones.

Es interesante notar que los típicos requerimientos del usuario no contienen información cuantitativa. La falta de esta información indica que algunos requerimientos están basados en la intuición. Parte del trabajo del diseñador es establecer cuál es un tiempo de entrega aceptable, qué nivel de seguridad es realmente necesario, cuál es el rendimiento predecible y qué tipo de tráfico debe ser protegido.

Se pueden realizar progresos a partir de este punto, teniendo en mente que hay algunos aspectos que deben ser refinados o negociados.

Diseño de la arquitectura

Una vez analizados los requerimientos, el diseñador comenzará a pensar en las posibles soluciones en forma abstracta. Este punto del análisis será en términos de los tipos de sitios genéricos que necesitan ser interconectados, en lugar de pensar en detalles a profundidad de sitios específicos.

El diseñador necesitará escoger una topología para enlazar los sitios entre sí de la manera requerida. Lo siguiente a establecer es cual tecnología (o tecnologías) es la más apropiada para satisfacer las necesidades. Como sucede en la mayoría de las redes, los cuello de botella de la información recaen en el equipo de frontera entre la red de área local y la red de área amplia (o inclusive red de gran escala).

Una red típica de área local en la UNAM opera a velocidades en el rango de 10-100Mbps. Estas tienden a soportar la carga generada por la mayoría de las aplicaciones de usuario. Por ejemplo, una LAN configurada para operaciones cliente/servidor en la cual los usuarios necesitan transmitir grandes cantidades de datos,

demanda un gran ancho de banda por periodos cortos de tiempo. En contraste, los enlaces de área amplia (o de gran escala) están orientados a una conexión semipermanente, en lugar de un ancho de banda variable. Al respecto, se necesitan los conocimientos técnicos que permitan al diseño tener un buen rendimiento global.

Es común en esta etapa esquematizar un número de posibles soluciones. Una rápida descripción de los escenarios puede ser hecha para reducir las posibilidades a uno o dos diseños e ir a la etapa de diseño de mayor detalle. Al comparar las tecnologías, los siguientes aspectos deben ser considerados:

- Costo comparativo de las tecnologías.
- Rendimiento (latencia y capacidad de transmisión).
- Confiabilidad.
- Áreas potenciales de riesgo (especialmente las propuestas para usar tecnología no probada).

Este análisis puede continuar para formar las bases de un registro de riesgos que debe ser mantenido a través del proyecto para administrar las fallas.

Es posible en esta etapa que identifiquemos la necesidad de un componente en el diseño para el cual no existe proveedor. Esto puede indicar en el estudio de viabilidad la posibilidad de trabajar en un desarrollo personalizado.

Diseño físico (Equipo activo)

Se refiere a los componentes físicos que tienen que ser adquiridos e instalados. Esto debe ser considerado en algún detalle en la primera etapa de diseño, ya que los componentes físicos son el mayor costo de capital para la red. También, los costos de mantenimiento y administración son generalmente calculados para el número y tipo de componentes usados en la red.

Se puede dividir este paso en diseño interior (redes de área local) y diseño exterior (redes de área amplia). En algunos casos las redes locales pueden ser conectadas directamente a la WAN, pero algún tipo de equipo interfaz se requerirá para conectar la LAN a la WAN.

Diseño del backbone

Esta red de área amplia es comúnmente representada como una nube y es fácil perder de vista que la red no es una cosa con recursos ilimitados. Cualquier red de alto desempeño impactará en la red WAN (o LAN a gran escala). Es decir, los nodos de red adicionales tendrán que permitir que la red pueda absorber a una larga y nueva generación de redes.

Va a ser necesario asegurar que hay suficientes puertos libres en el equipo. Si esta condición no se cumple, se debe planear la apropiada expansión de la red. También se debe asegurar que existe la adecuada capacidad en los diferentes enlaces, demostrar como se va a monitorear su utilización y que acciones pueden ser tomadas para incrementar el ancho de banda si se necesita.

Diseño lógico (Configuración)

Este aspecto del diseño concierne a la configuración de los componentes, y como interactúan como un sistema para proveer servicios de punta a punta. Las áreas de consideración son el diseño de esquemas de direccionamiento, métodos de ruteo y como se va a recuperar la red bajo condiciones de falla. Los principios del diseño lógico deben estar completamente establecidos en las primeras etapas para confiar que el diseño propuesto y seleccionado funcione.

Diseño de la administración

La calidad de servicio proporcionada por la red de alto desempeño será tan buena como lo sea el sistema de administración que exista para soportar las aplicaciones. El diseño de estos sistemas incluye aspectos físicos (equipo y ubicación) y lógicos (alarmas y procedimientos). Los aspectos físicos del sistema de administración

necesitan ser establecidos en las primeras etapas del proceso de diseño para que el costo implicado se pueda anexar al estimado total.

Verificación y validación

La verificación consiste en hacer cálculos, pruebas y demostraciones para establecer que el diseño cumple con los requerimientos del usuario.

La validación es la prueba formal de que la red instalada satisface los requerimientos. Esta consiste en la presentación de pruebas hechas en laboratorio y conforme se agreguen nuevos nodos a la red.

La verificación y validación son pasos clave para entregar una red bajo un sistema formal de control de calidad (ej. ISO 9001).

Las necesidades del usuario (expresadas en términos de los servicios que quieren) ahora deben mostrarse viables a través de las tecnologías seleccionadas. Uno de los primeros aspectos de esta verificación es comprobar que el tráfico requerido puede ser soportado. Esto es un poco más complicado de lo que parece. El principal problema con la estimación del tráfico es que el usuario rara vez sabe cuales son sus requerimientos. Tal vez la mejor forma de lidiar con esto es trabajar en los escenarios y presentar los tráficos estimados. Esto puede ser hecho observando los niveles de tráfico en la red existente y aplicar reglas de diseño para saber la capacidad requerida por la nueva red. Ejemplos para la estimación de tráfico pueden ser:

- En un día promedio, hay 5000 transferencias de archivo desde el sitio 1 hacia los sitios 2 y 3, y 2000 en el sentido opuesto.
- El resto del tráfico por la transferencia de archivos es esporádico y de niveles muy bajos: puede ser ignorado.
- Los archivos enviados desde un sitio hacia otro son de 25kbytes en promedio.
- Las descargas de la base de datos maestra se realizan a las 11:00 de la noche. Toman una hora y son típicamente de 50Mbytes.
- El tráfico de correo entre sitios es sumamente bajo, puede ser ignorado.

Hasta ahora, se puede tener cierta confianza de que la red propuesta está encajando en los propósitos establecidos. El diseño debe ser lo suficiente rápido para satisfacer las necesidades del usuario, pero no sobreestimado (y en consecuencia, demasiado caro). El siguiente paso es transportar el plan lógico al físico para que el equipo y servicios que pueden hacerlo realidad sean procurados e instalados.

Cada opción tendrá sus ventajas y desventajas. Las características principales que afectan en la decisión final son:

- Retraso.
- Seguridad.
- Administración.
- Costo.
- Flexibilidad.

Operación y evolución

Una vez que la red ha sido diseñada, instalada y probada, pasará a la etapa de operación. En esta etapa es poco probable que permanezca estática. El diseñador tendrá que administrar constantes cambios en la red. El cambio puede ocurrir por varias razones, incluyendo:

- Solución de fallas en la red (ej. aplicaciones, equipo o diseño).
- Incremento del tráfico.
- Cambio en los requerimientos.

Esta evolución post-operacional puede, en lo razonable, ser prevista en el diseño inicial. Es cierto que las fallas ocasionadas por los inevitables cambios resultan en redes que rápidamente se convierten en una inconveniencia en lugar de una ventaja. Estos pasos son secuenciales y resultan en un diseño de red que, una vez implantado y con las debidas reservas, hace exactamente lo que el usuario pidió en primera instancia. Es común encontrar puntos sin solución, decisiones precipitadas, cambios o requerimientos erróneos y en tal caso, se tiene que comenzar de nuevo en una etapa previa en el proceso. Las actividades mencionadas deben ser vistas como elementos de un ciclo de vida interactivo, si un paso falla, se debe regresar al paso válido anterior. Al trabajar en el costo total de la red se debe cubrir el capital y los gastos actuales y debe cubrir gastos secundarios como actualizaciones en software y hardware, mantenimiento, licencias y contratos de servicio.

Un punto más en los procesos descritos es que cubre solamente los procesos de diseño. Tópicos como la administración y la solución de problemas deben ser incluidos en el diseño de cualquier red.

2.3. Requerimientos tácticos y técnicos

Los requerimientos tácticos se encuentran cuando se platica con los usuarios —las personas que realmente utilizan los servicios. Estos requerimientos son relativamente sencillos de explicar basados en los problemas que los usuarios tienen y que deben ser solucionados por la red. Por ejemplo:

- Transferir un archivo de A hacia B toma mucho tiempo.
- El camino de C a D es poco confiable.
- Tenemos correo electrónico en este departamento pero no podemos comunicarnos con otras personas: es incompatible.
- Los sistemas existentes no pueden ser reemplazados y deben ser soportados por la nueva red.

Los requerimientos técnicos podrían ser:

- Listado de sitios y direccionamiento a considerar.
- Documentación de la red existente.
- Estadísticas de tráfico de la red actual.
- Estimado de niveles de tráfico para las nuevas aplicaciones.
- Recursos necesarios para las distintas aplicaciones de red.
- Capacidad y latencia necesaria para las aplicaciones.

Al conocer la infraestructura existente se podrán entender las aplicaciones y sistemas que necesitan ser soportados, así como los patrones de tráfico que estos generan. No es una tarea simple, pues la documentación de los sistemas existentes y sitios puede ser escasa y se requiere de mucho trabajo para completarla, sin embargo, puede revelar las causas de los problemas que los usuarios experimentan, como un bajo rendimiento o cuestiones de confiabilidad.

Conectar un analizador de redes a segmentos existentes puede ser muy relevante. Muchas aplicaciones son diseñadas asumiendo que operan sobre un segmento de red local corriendo a 10 Mbps. Con esta relativamente amplia capacidad, las aplicaciones pueden ser algo ineficientes en el uso del ancho de banda, enviando muchos mensajes entre cliente y servidor para lograr las tareas más simples. Cuando cliente y servidor son separados por un enlace corriendo a 64 Kbps las aplicaciones se desempeñan aun peor. Algunos análisis a la red pueden ser necesarios para establecer información cuantitativa como el tamaño de los mensajes, volúmenes de tráfico y tiempo de transacciones completadas.

Por supuesto, en algunos casos, no habrá una red existente. Este puede ser el caso de áreas de reciente creación o lugares en donde se adopta de manera tardía la tecnología de la información. En muchos sentidos es más fácil para el diseñador crear una solución donde no existe una red previa, ya que no se requieren algunas consideraciones como la integración o migración de tráfico. Por otro lado, un área que no ha utilizado este tipo de tecnología no tiene una idea clara del flujo de tráfico que generará una vez que la red se vuelva

operacional. En este caso, el uso de prototipos y escenarios se vuelve realmente importante. Cualquier cosa que permita un acercamiento a la tecnología es útil.

2.4. Planeación para el futuro

Las redes de alto desempeño exitosas serán aquellas con suficiente flexibilidad y agilidad para evolucionar y satisfacer los constantes cambios en los requerimientos de sus usuarios. Si se ha logrado diseñar una red eficiente, el tráfico tiende a crecer y eventualmente poner a prueba la capacidad. Así como crece el tráfico, el diseñador va a ser requerido para efectuar modificaciones conforme los sistemas y la tecnología cambien.

Una medida esencial de la calidad de la red es su habilidad para cambiar y satisfacer nuevos requerimientos. Estos pueden ser generados por mejoras en la tecnología, por demandas para una mejor funcionalidad o por cambios o expansión del área a la que se proporciona servicios. Cada uno de estos factores impacta en la red y debe ser previsto en el proceso de diseño.

2.4.1. Administración del cambio

Un requerimiento obvio es mantener el control sobre los cambios en la red. Es muy fácil para cualquier administrador de red agregar un servidor o un segmento LAN, que puede resultar en consecuencias imprevistas en la red como conjunto. Las redes modernas pueden ser bastante grandes y complejas. Su correcta operación depende de tener cuidado de asegurar que las reglas de interacción del diseño no sean excedidas.

La experiencia ha demostrado que algunos de los (aparentemente inocentes) cambios, como agregar un nuevo grupo de hubs en la red puede traer consecuencias desastrosas. Este equipo extra puede ocasionar que los límites de apilamiento de los equipos sean excedidos, o que se incremente la cantidad de información que otros equipos en la red tienen que mantener y procesar. Como resultado, la red puede hacerse inestable y fallar por completo.

Aún los proveedores generan cambios frecuentes y rápidos ocasionando que la documentación del diseño no esté actualizada, comprometiendo la habilidad de administrar la red efectivamente. Un proceso formal para controlar los cambios en la red debe ser instaurado como una parte integral de los esquemas de administración de la calidad.

Los cambios en la red pueden ocurrir no solo como resultado de los requerimientos del usuario, también de las especificaciones del proveedor. Siempre habrá conflicto entre la necesidad de hacer cambios en la red y la necesidad de mantener la estabilidad operacional, debido a que el objetivo final es que los usuarios puedan explotar las aplicaciones que la red pretende soportar. Una forma de manejar esto es tratar a la red en forma muy similar a un proyecto de software en el sentido de que no es deseable presentar una nueva versión para cada cambio. Es simplemente muy caro y trastornante hacer cambios tan frecuentes, ya que cada uno necesitará del proceso completo de desarrollo.

La posible respuesta es practicar el control de versión en el diseño de red. Una plan de versión es producido, mostrando cuales cambios deben ser realizados en que elementos. Las ventajas son:

- Los trastornos y gastos son minimizados.
- Se puede describir precisamente el estado actual de la red en términos de un número de versión en el diseño.
- La documentación puede ser cambiada y revisada para reflejar cada versión, y marcada con un número para mostrar la fecha más reciente de la documentación que estamos usando.
- Es más fácil planear una clara estrategia técnica que pueda concordar con el usuario para definir el diseño de las versiones.
- Es más fácil prioritizar y calendarizar cambios.

Se sugiere, como mínimo, un número de versión que conste de dos partes en el cual, el primer número de izquierda a derecha cubre cambios significativos en la red. Estos pueden ser:

- Fases del ciclo de vida —red experimental, red piloto.
- Expansión a gran escala —incremento de usuarios en más del 50%.
- Agregado de nuevos sitios.
- Cambio en la tecnología de backbone.
- Actualización de software en el equipo activo.

Y el segundo cubre cambios menores:

- Cambio de equipos secundarios, inclusive no activos.
- Adición de un número pequeño de usuarios.
- Actualizaciones menores de software.

Al crear las versiones e implantar los cambios requeridos para una nueva versión, el diseñador de red tiene que hacer un fino balance entre los siguientes consideraciones:

- Asegurar que los cambios son realizados lo suficientemente rápido para responder a las necesidades del usuario.
- Mantener la estabilidad en la red.
- No hacer muchos cambios en una sola sesión.

2.4.2. Revisión del diseño

Claramente, el cambio puede ser manejado si sabemos que va a suceder, y podemos planearlo. Nada es peor para un administrador de red que recibir una petición de cambio demandando que un nuevo servicio sea instalado a la brevedad posible.

Una forma efectiva de anticipar el cambio es mantener revisiones periódicas al diseño con administradores de red y desarrolladores. Estas revisiones tienen dos ventajas:

- Establecer que la red está respondiendo a los requerimientos existentes.
- Establecer cualquier requerimiento futuro.

Cuando se ven los requerimientos actuales, debemos determinar si todos los requerimientos cuantitativos están solucionados. El sistema de administración debe proporcionar la evidencia necesaria para investigar cada planteamiento. Estas revisiones deben ser vistas como una oportunidad para vislumbrar los cambios. Algunas de las principales áreas a checar son:

- La tendencia que tendrá el tráfico tomando como referencia el actual.
- Crecimiento esperado del tráfico debido a aplicaciones existentes.
- Nuevos sitios o usuarios a conectar.
- Nuevas aplicaciones en desarrollo.
- Identificar las estrategias que puedan tener influencia en la red.

Los cambios requeridos en la red deben ser reconsiderados en el aspecto económico. Las actualizaciones a la red invariablemente involucrarán costos adicionales, que deben ser justificados. Si no existen los recursos necesarios para llevar a cabo todos los cambios identificados, entonces tendrán que ser priorizados. Alternativamente, los diseñadores pueden identificar otros métodos para lograr los mismos objetivos.

2.4.3. Aplicaciones multimedia

Dado que la comunidad de usuarios no tiene claro la forma que tomaran las futuras aplicaciones, vale la pena especular. Por ejemplo, ha habido mucho progreso en lo referido a multimedia y se incrementa el

número de usuarios que cuentan en su estación de trabajo con los periféricos apropiados para soportar estas aplicaciones:

- *Transferencia de imágenes.* Las estaciones de trabajo ahora son capaces de desplegar imágenes a color de alta calidad. También tienen el poder de procesamiento para manejar las técnicas de compresión que hacen posible almacenar imágenes de alta calidad en archivos de tamaño razonable (ej. formatos TIFF o JPEG). Es posible almacenar estas imágenes en una base de datos y acceder remotamente.

- *Comunicación interpersonal.* Los usuarios están requiriendo que sus redes soporten las facilidades del audio y el video para reemplazar la telefonía tradicional y proveer videoconferencia. En el presente, muchos usuarios tienen separado este tipo de tráfico en redes dedicadas. La tecnología está evolucionando rápidamente y permite que este tipo de tráfico sea transportado sobre la red de alto desempeño.

  El argumento es que la voz o el video digitalizado es solamente otro tipo de datos, y se puede explotar la holgura en la capacidad de las redes de datos para transportar este tráfico. También facilita el uso de tecnologías como "soft PABX" (plataformas basadas en PC que permiten remplazar los costosos PBX) y la integración de la telefonía en la computadora.

  Una tecnología emergente es voz sobre IP (VoIP). Funciona enviando las muestras de voz codificadas digitalmente a través de la red como paquetes IP. Un aspecto clave de esta tecnología es que es muy sensible a la latencia y sus variaciones. La latencia puede solventarse empleando técnicas de almacenamiento en memoria (buffering).

  Para hacer funcionar VoIP, se necesita una red con un gran ancho de banda y mucha capacidad disponible (para asegurar que la latencia se mantenga lo más bajo posible) o una red que tenga arreglos para implementar alguna forma de calidad de servicio (QoS). Esto asegura que las muestras de voz sean enviadas por la red con mayor prioridad que el tráfico de datos. Los resultados de esta tecnología pueden ser variables, y se recomienda ser cuidadoso al momento de probarla, ya que si se enfatiza en que la calidad sea la adecuada, se pueden descuidar transacciones de misión crítica e impactar su rendimiento.

2.4.4. Diseño para la migración

Al instalar la red de alto desempeño propuesta, una gran parte del diseño se enfocará en la migración de la red existente. Del mismo modo, las redes de ahora se convierten en el legado del futuro —y si tenemos alguna estrategia para definir la forma que tendrá la red del futuro será posible facilitar tal migración. Algunas ideas para las estrategias de migración son:

- *Funcionamiento en paralelo.* Durante el periodo de migración, existirá la necesidad de que las nuevas tecnologías coexistan con las viejas.

- *Minimización del costo.* Es deseable que el costo de la migración sea lo más bajo posible, y que el retiro del equipo viejo sea lo más rápido. Un motivo para cambiar a una nueva tecnología es que el mantenimiento de sistemas obsoletos es alto.

- *Preparación técnica.* Puede ser posible anticipar las necesidades de las nuevas tecnologías. Usualmente las nuevas versiones de software requieren más memoria que las actuales.

- *Compatibilidad.* Actualizar una red se puede volver difícil si las nuevas versiones del equipo activo y el software son incompatibles con las versiones actuales. En el caso contrario, las redes pueden ser actualizadas en forma gradual sin requerir que los tiempos de desconexión del servicio sean altos.

A parte de estos factores, hay otras complejidades como transferir información importante de una red a otra. Un punto clave que ayuda a solucionar los puntos anteriores es saber exactamente que es lo que se tiene, es decir, contar con un inventario de los componente de la red, usuarios, información y servicios.

2.5. Verificación, validación, pruebas y operación

La concepción tradicional de probar es la actividad inmediata anterior a la liberación del producto terminado. Idealmente, debe ser asociado con todas las etapas del diseño y debe lidiar con la validación de los requerimientos y la verificación de las especificaciones así como las mediciones y pruebas al producto tangible. La idea de checar conforme al progreso es que es mucho más barato y fácil remover un problema en la etapa de creación del diseño, que reconfigurar una red instalada y operando.

Ninguna cantidad de pruebas garantizará un resultado libre de errores. La complejidad de las redes modernas indica que siempre habrá algunas fallas operacionales o características no vislumbradas que resulten en acciones correctivas necesarias.

2.5.1. Verificación

Es esencial que durante el proceso de diseño, se lleve a cabo la verificación. Consiste en una serie de argumentos, cálculos y demostraciones que ayuden a demostrar que el diseño cumplirá con los requerimientos establecidos por el usuario.

2.5.1.1. Declaración de conformidad

Tal vez la forma más simple de verificación. Es usualmente presentada en forma tabular, con columnas como sigue:

- *Requerimiento*. El número de referencia para el requerimiento. Es proporcionado acompañado de una breve descripción.
- *Declaración de conformidad*. Es usualmente una palabra o frase, por ejemplo: aceptado, no aceptado, imparcial.
- *Justificación*. Será algún texto explicando por que el diseño cumple o no con el requerimiento. Cuando existe una no-aceptación, debe darse una propuesta alterna para lograr el objetivo.

2.5.1.2. Riesgos

En algunas ocasiones, las peticiones están basadas en algún grado de suposición. Esto puede ser información sobre-entendida, basada en experiencia, para cubrir lagunas en los requerimientos. Puede ser el supuesto de que ciertas características no probadas de un equipo funcionen correctamente. En dado caso, un registro debe ser hecho para cada riesgo, indicando el impacto en la red si llega a ocurrir. También se debe crear un plan concerniente a los pasos establecidos para minimizar el riesgo. Las áreas administrativas querrán ver un estimado económico para cada riesgo —cuánto costará hacerlo funcionar y cuánto pagar en daños.

2.5.1.3. Cálculos

Una serie de cálculos serán requeridos para respaldar las peticiones hechas en la declaración de conformidad. Se presentan algunos de los métodos más comúnmente utilizados por los diseñadores cuando se lleva a cabo el trabajo de verificación.

Latencia en la red

La latencia en la red es un factor clave para determinar la calidad del servicio (QoS) experimentada en las aplicaciones orientadas a la transacción. Los cálculos para el retraso normalmente se requerirán en base a la eficiencia.

Es particularmente importante que un entendimiento generalizado de la latencia se tenga en mente, incluyendo el inicio y fin de la medición, que incluye y que tan largos son los mensajes. Una buena definición

podría ser: "la latencia es el tiempo a partir del cual el primer bit de un mensaje de petición de 128 octetos de una aplicación deja el origen hasta el momento en el que último bit de los 2048 octetos del mensaje de respuesta es recibido en el destino". La figura 2 muestra un escenario de red típico y los elementos del retraso que deben ser considerados.

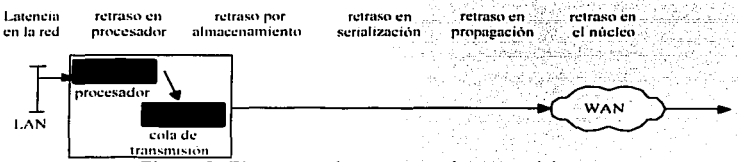


Figura 2. Elementos de retraso en la transmisión

Retraso en propagación

Este elemento de retraso es causado por el hecho de que las señales viajan a una velocidad finita. La velocidad va a ser disminuida porque la señal no va a tomar el camino más corto posible, las señales se propagan más lento en cables o fibra óptica que en el vacío y el equipo activo añade retraso extra en el camino. Generalmente, no vamos a saber el camino exacto que sigue el cable y solo sabremos la distancia lineal entre los extremos. El retraso en la propagación se vuelve importante al trabajar en entidades regionales, en enlaces internacionales y cuando las aplicaciones requieren un retraso mínimo para funcionar adecuadamente [bib04].

Retraso por almacenamiento

El procesador en cada nodo de red (ej. un switch o router) tomará una cantidad de tiempo finita para analizar cada paquete y determinar como enrutarlo. Este retraso (generalmente pequeño) puede ser encontrado en las especificaciones del fabricante o puede ser determinado por mediciones en laboratorio. Si es un dispositivo simple con un solo procesador, es recomendable asumir que los paquetes son procesados uno a la vez y en consecuencia el recíproco del envío de paquetes por segundo es una buena indicación de la latencia.

Si los usuarios LAN envían una ráfaga de paquetes hacia un destino remoto, el circuito de acceso WAN formará un cuello de botella. Los paquetes tendrán que ser almacenados y esperar su turno. Esta es un área especialmente importante de retraso, porque es la que introduce la mayor variabilidad dentro del retraso total en la red. Algunas aplicaciones (especialmente aquellas involucradas en el transporte de información de voz o video en tiempo real) son particularmente sensibles a variaciones en el retraso. Los usuarios de transacciones interactivas por computadora también notan retrasos variables, y esto puede afectar su productividad.

Throughput

Esto es particularmente importante para aplicaciones de transferencia de archivos. El usuario necesitará una garantía del nivel de throughput para la transferencia de archivos que puede ser sostenido.

La limitación principal del throughput va a ser el enlace más lento en la ruta de conexión de dos extremos a través de la red. Aun cuando un sistema final sea conectado a Ethernet 10Mbps, la transferencia de archivos no puede exceder 65Kbps si esa es la velocidad del circuito de acceso usada para conectar el sitio remoto en la red.

Para calcular el throughput, también necesitamos comprender el protocolo de transferencia del usuario para la comunicación punta a punta. Estos protocolos trabajan enviando bloques de datos y después esperando por un acknowledge (acuse de recibo). Generalmente, el protocolo permitirá más de un bloque de datos para enviar sin recibir un acuse. La máxima cantidad de datos que puede ser enviada sin un acuse es referida como ventana. Necesitamos saber el tamaño de la ventana y el tamaño de cada bloque enviado. Es común en esquemas de ventana que el sistema origen envíe un grupo de paquetes y después tenga que esperar a que sea

propagado por la red. No se pueden enviar más datos hasta que un bloque de datos haya sido recibido en el destino y un acuse haya sido enviado y recibido. La figura 3 muestra un sistema con un tamaño de ventana de 2.

Cuando el cierre de la ventana es normal, el throughput está fuertemente influenciado por el retraso total en la red. Lo más rápido que un acuse pueda ser recibido en el diagrama es después de que el bloque 1 haya sido recibido y el acuse se haya propagado de regreso al origen. Bajo estas circunstancias:

v = circuito con menor velocidad
t = tiempo para enviar una ventana de datos
ta = tiempo para recibir el primer acuse

Throughput = v * (t / ta)

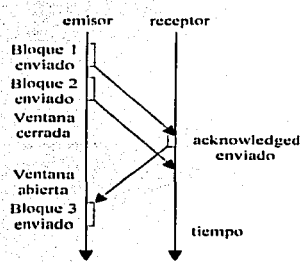


Figura 3. Sistema de ventana para la transmisión

Idealmente, el usuario debe ajustar sus parámetros de transferencia de archivos para mantener la ventana abierta. Note que el protocolo de Internet FTP hace uso del protocolo de transporte TCP. Este desarrolla un mecanismo de "sliding window". Cuando la sesión de TCP es abierta, comienza con una ventana pequeña. Conforme las transferencias son exitosamente completadas, TCP incrementa gradualmente el tamaño de la ventana. Este proceso continua hasta que la red comienza a congestionarse. En este punto, podemos esperar que la red comience a perder paquetes. Una vez que la sesión de TCP comienza a retransmitir, debido a paquetes perdidos, reduce significativamente el tamaño de la ventana, ayudando a prevenir más congestiones en la red. Los diseñadores deben ser cuidadosos con este comportamiento. Esto quiere decir que los procesos concatenados de transferencia de archivos intentarán tanto ancho de banda como sea posible, y pueden impactar severamente cualquier tráfico orientado a transacciones que este compartiendo la red. La solución es utilizar técnicas de prioritización de tráfico para restringir el ancho de banda disponible para el protocolo FTP, asegurando que el tráfico orientado a transacciones obtenga una compartición justa.

Las redes de datos también están expuestas a los errores de línea. Típicamente los enlaces análogos pueden tener una taza de errores de un bit cada 100 000 en promedio. En un enlace digital puede corromperse un bit por millón. Cuando hay un paquete incompleto en la red, será descartado debido a una comprobación de errores en la capa de enlace, o por una comprobación en la cabecera de TCP. El protocolo TCP detecta la pérdida, y solicita que éste sea retransmitido —reduciendo el throughput útil. Para la probabilidad de pérdida de paquetes por errores en la línea, necesitamos añadir la probabilidad de pérdida de paquetes debido a que sean descartados por el equipo activo. Con TCP/IP, el estándar para manejar la congestión en la red es simplemente descartar los paquetes excesivos. El diseñador de red diseñará el núcleo de la red para que la congestión sea minimizada. El protocolo TCP detectará y se recuperará de la pérdida de paquetes. Entre más paquetes tengan que ser reenviados para recuperar los perdidos, peor va a ser el throughput útil.

Bloqueo

Este cálculo aplica en un situación en la que los sistemas de usuario se conecten bajo demanda a sistemas de servidores. Por ejemplo personas que realizan acceso telefónico a puertos de acceso, o enlaces con respaldo vía módem alrededor de la red principal.

En algunos casos, cuando un usuario se va a conectar por largos periodos y debe garantizarse su conectividad, será apropiado dedicar un puerto de acceso al usuario. Sin embargo, generalmente, esto no es costeable, y los usuarios deben competir por un número limitado de puertos. En este caso, es normal aprobar una taza de bloqueo, por ejemplo, que porcentaje de llamadas en la hora pico van a fallar para encontrar un servidor de acceso libre.

La industria de la telefonía tiene un modelo útil que puede ser utilizado para cálculos de bloqueo. Primero, determina el mayor nivel tráfico que se espera recibir en la red. Esto se define como la suma de la duración de todas las llamadas, dividido entre el periodo en el cual las llamadas ocurren —comúnmente descrito como el número de llamadas por hora. Dado el nivel de tráfico y el número de puertos disponibles, uno puede calcular la taza de bloqueo. Alternativamente, dada la taza de bloqueo requerida, se puede estimar el número de puertos necesarios.

Disponibilidad

Una definición típica para esto puede ser la probabilidad, en cualquier momento, de que un nodo principal sea capaz de comunicarse exitosamente con un sitio remoto.

Esta disponibilidad puede ser calculada dados los componentes conocidos para la disponibilidad (ej. switch, conexión de red, línea ISDN, etc.). Estos componentes están dispuestos dentro de una cadena de disponibilidad, representando la tecnología propuesta de red, siendo entonces viable su cálculo. La disponibilidad es dependiente del MTBF (mean time between failure) y el MTTR (mean time to repair).

$$\text{Disponibilidad} = \text{MTBF} / (\text{MTBF} - \text{MTTR})$$

Para componentes de red bien establecidos, es esperado que el MTBF se derive del historial de fallas. Para nuevos componentes, el MTBF puede ser derivado a través de cálculos, basados en la disponibilidad conocida de los subcomponentes [bib04]. El diseñador de red siempre debe entender las bases para cualquier declaración de disponibilidad, y formar una opinión de que tan preciso puede ser.

El MTTR es una medida muy importante para el usuario, dado que es una cláusula clave en la prestación de servicios. Al acordar niveles de disponibilidad, es importante considerar que periodo del día debe ser medido —típicamente, una alta disponibilidad es requerida durante las horas de trabajo en lugar de fines de semana. Cuando una conexión de red es de misión crítica y necesaria a cualquier hora, el usuario usualmente requerirá un MTTR de 4 horas, provisto las 24 horas del día los 365 días del año. Las conexiones menos críticas solamente pueden requerir reparaciones durante 8 horas de trabajo (lo cual significa que el servicio sea reparado al siguiente día hábil).

La disponibilidad de punta a punta de un enlace dentro de la red de alto rendimiento necesita tomar en cuenta todos los diferentes componente por los cuales la información tiene que pasar, y cualquier enlace de respaldo que haya sido provisto. Los componentes de disponibilidad son combinados y mostrados en la figura 4.

El diseñador de red necesita comprender que una falla es un proceso aleatorio, y que los cálculos de disponibilidad están basados en un proceso estadístico. El valor predictivo de los cálculos es lo mejor que se puede hacer cuando se lidia con redes de gran escala.

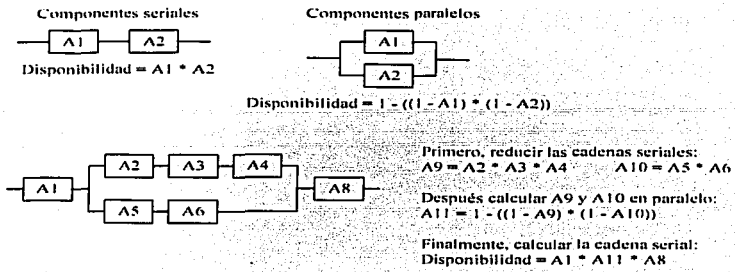


Figura 4. componentes de disponibilidad para una red de alto desempeño

2.5.2. Validación

Si la verificación consiste en checar que se está trabajando de la manera correcta (al menos en teoría), la validación trata de asegurar que la teoría se traslade a la práctica como se desea. En muchos sentidos, es una cuestión en la que hay que estar familiarizado con los elementos de diseño utilizados y con las cuestiones que surgen en el desarrollo de sistemas y la operación de las redes.

Componentes

Con cambios tan rápidos en la tecnología, es cierto que se van a utilizar componentes en el diseño de las redes que son nuevos (o quizá aún en desarrollo). Productos, como los routers, también están en un continuo estado de innovación, con liberaciones de software sucediendo de dos a cuatro veces por año. Las liberaciones son empacadas con nuevas características algunas de las cuales pueden estar contempladas en el diseño. Desafortunadamente las nuevas características pueden presentar incompatibilidades así que es altamente recomendable probar cualquier tecnología que se intente usar.

Es inevitable que, durante las primeras etapas del diseño, un número de suposiciones van a tener que ser hechas acerca de la operación y el rendimiento de los componentes. Es buena idea probar las suposiciones en la misma etapa.

Antes de confiar las aplicaciones críticas a estas tecnologías, son esenciales las pruebas piloto a pequeña escala. Estas deben ayudar a:

- Probar que la tecnología funciona.
- Integrar los componentes de la red con los sistemas finales.
- Mostrar que ofrece un rendimiento aceptable.
- Demostrar su confiabilidad.
- Entrenar en la nueva tecnología.
- Recabar la información requerida para la implementación del diseño.
- Validar las suposiciones del diseño.

Laboratorio de pruebas

Es recomendable en cualquier implementación establecer un laboratorio de pruebas permanente. Es deseable que las conexiones de red más importantes y el equipo activo asociado sean añadidos al laboratorio, para que la red pueda ser integrada con los sistemas finales y las aplicaciones.

Una vez asentados los planes para instalar el laboratorio, el siguiente paso será diseñar un conjunto de pruebas de integración y aceptación que puedan ser usadas para probar que las aplicaciones del usuario operarán

satisfactoriamente sobre la red propuesta. El proceso de diseño también tiene que sugerir una serie de pruebas para verificar las suposiciones referentes a la funcionalidad y el rendimiento de los componentes de red.

Cuando las pruebas son realizadas, es importante asegurar que los resultados queden perfectamente documentados, y la información cuantitativa obtenida sea incluida en el proceso de diseño.

Integración

Antes de que las pruebas a las aplicaciones puedan comenzar, es necesario integrar los componentes del laboratorio de pruebas. Una vez instalados e interconectados, deben ser configurados, y la conectividad básica verificada.

Es altamente recomendable que la integración se realice paso a paso. Si tratamos de obtener el sistema funcionando en una sola sesión, puede ser difícil y tardado resolver los problemas que lleguen a ocurrir.

El diseño lógico tiene que proveer las directivas adecuadas para la configuración de los componentes del laboratorio, pero dicho documento debe ser revisado para realizar las modificaciones necesarias.

Durante las pruebas, es sabido que los problemas aparecerán, y la disciplina esencial para identificarlos y resolverlos será desarrollada.

Pruebas y demostraciones

La importancia de las pruebas no puede ser subestimada —aun los mejores planes, implementados de manera correcta, tienen la posibilidad de fallar. Así como se tiene que probar la funcionalidad y el rendimiento de la red propuesta, un papel clave del laboratorio de pruebas será asistir en la puesta a punto de la red para mejorar el rendimiento. No siempre será posible determinar la configuración más optima durante el proceso de diseño, y probablemente se necesite determinar experimentalmente, o en el laboratorio. Las áreas en las cuales se requiere de optimización son:

- Ventanas y tamaño de los paquetes.
- Priorización.
- Parámetros de los protocolos de ruteo.
- Asignación de almacenamiento para el tráfico.

Un punto muy importante a recalcar es que el trabajo de validación, verificación y pruebas nunca se termina. La idea de estos pasos a través del diseño es reducir el riesgo de falla y las características más importantes son:

- Especial atención en los sistemas existentes.
- Dificultades al calendarizar el tiempo y los recursos necesarios para realizar las pruebas.
- Problemas para obtener el equipo de pruebas adecuado.
- Probar las combinaciones de protocolo y aplicaciones.
- Pruebas con la máxima carga de trabajo.

2.5.3. Solución de problemas

La tecnología utilizada en las redes modernas evoluciona rápidamente, y muchos de estos sistemas pueden ser relativamente inmaduros. Es casi inevitable que el usuario pueda experimentar algunos problemas significativos en la red, especialmente en los primeros días.

Además del involucramiento directo con la detección de fallas, el diseñador de red también va a estar inmiscuido en diseñar los sistemas y procesos de administración. Esto origina que sea proactiva la detección de errores y, en lo posible, automática su solución.

Los pasos recomendados para la solución de problemas son los siguientes:

- *Identificar el problema — Reactivo vs. Proactivo.* Los problemas en la red se vuelven evidentes a los usuarios cuando sus aplicaciones dejan de comunicarse u operan con un rendimiento degradado. Una vez que el usuario ha notado el problema, lo reportará al administrador de red. Esto es identificación reactiva. Este planteamiento es satisfactorio para las aplicaciones más comunes, sin embargo algunos usuarios prefieren una identificación proactiva. Es cuando los sistemas de administración de la red son capaces de detectar la falla antes que el usuario, permitiéndole al administrador de red comenzar con la solución de la falla antes de que el usuario reporte el problema. (Idealmente el diseño de red automáticamente se recuperará después de varias fallas indicando el momento en que sea necesaria la reparación).

- *Evaluar el impacto y registrar el problema.* Por instinto se tratará de remediar el problema lo más rápido posible. Cuando se lidia con una red de alto desempeño a gran escala, donde varias fallas se pueden presentan simultáneamente, una mayor disciplina es requerida. Lo primero va a ser registrar el problema y determinar su prioridad. El operador de la red debe ser apoyado por una herramienta automática de registro de fallas. Esto permitirá que la falla sea almacenada en una base de datos, junto con los subsecuentes reportes de progreso y los detalles de la falla, así como estadísticas abarcando la periodicidad de las fallas y el tiempo necesario para resolverlas.

- *Operación de emergencia.* Modo de operación hasta que la situación regrese a la normalidad, y puede variar con el tipo de desastre y su respuesta. Es difícil establecer la efectividad de este paso por lo que hay que estar preparados para realizar cambios inmediatos.

- *Recabar las evidencias.* Muchas de las fallas que ocurren en la red son rutinarias por naturaleza. Es útil realizar un análisis de las fallas que involucre una distribución de las causas, ordenadas por su frecuencia de aparición. Al hacer este análisis, uno puede escoger entre mirar la frecuencia de repetición de la falla o el nivel de interrupción que ocasiona.

- *Reproducir la falla.* La situación ideal es que los mecanismos que originaron la falla sean los suficientemente entendidos para que pueda ser completamente reproducida en el laboratorio. Cuando la falla es reproducida, se puede enfocar el trabajo en establecer exactamente que componente(s) en la red ocasiona el problema.

- *Implementar la solución.* La solución es manejada en la misma forma que cualquier mejora en la red. Es implantada progresivamente después de cuidadosas pruebas, aunque puede haber presión por solucionar la falla rápidamente. Una vez que la solución ha sido identificada, es necesario demostrar que el problema ha sido solucionado en su totalidad por lo que las pruebas en el laboratorio son recomendables.

El problema de estas recomendaciones es que son difíciles de cuantificar al inicio de un proyecto. Generalmente, los problemas y limitaciones aparecen una vez que la red ha sido instalada y se encuentra en operación.

Uno de los retos más grandes a enfrentar por el diseñador es lidiar con tal grado de complejidad. Las características descritas solamente pueden ser logradas si el diseño propuesto ofrece la facilidad de analizar cada uno de sus componentes. Una forma para alcanzar dicho objetivo es manejar diferentes niveles de detalle o diferentes puntos de vista al momento de presentar el diseño. Es recomendable generar una lista de necesidades y la propuestas respectivas para justificar/defender las decisiones que se tomen.

Capítulo 3. Diseño físico y lógico

Muchas de las decisiones tomadas tempranamente en el proyecto tendrán un impacto significativo en la forma y calidad del producto final. El diseñador tiene un rol muy importante en este punto. Debe asegurar que la transición de los requerimientos a la red real este sólidamente basada. Lo que significa que los diseños de alto nivel deben ser alcanzables, prácticos y apropiados.

3.1. Arquitectura de las redes de alto desempeño

El objetivo del diseño de red durante la etapa de arquitectura es establecer y documentar una vista de alto nivel de la red propuesta, con suficiente nivel de detalle para:

- Establecer y documentar el acercamiento a la arquitectura a usar en la solución.
- Demostrar que el diseño cumplirá con los requerimientos del usuario.
- Permitir que el costo del diseño sea estimado con razonable exactitud.
- Identificar las mayores características que necesitan investigación y resolución antes de la implementación.

El énfasis principal por el momento será en los aspectos físicos del diseño, y los métodos necesarios. En esta etapa del proceso de diseño, se deberá pensar en una visión abstracta de la red. La figura 5 muestra una red típica con las siguientes características:

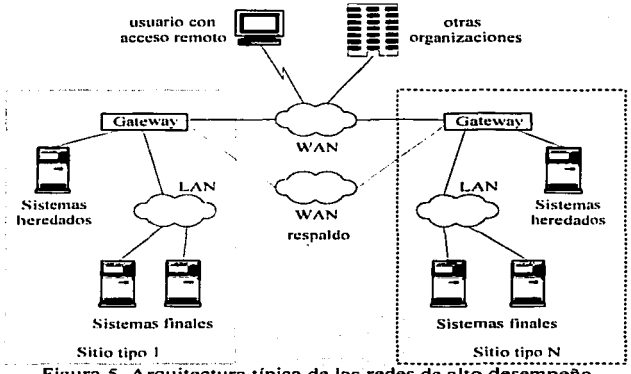


Figura 5. Arquitectura típica de las redes de alto desempeño

- *Tipos de sitios genéricos.* Un diseño de red eficiente ayudará, en lo posible, a tener un número pequeño de tipos de sitios. Así, puede diseñarse una solución para cada sitio, repitiéndolo tantas veces como sea necesario.

- *Sistemas finales.* Ultimamente, son las aplicaciones corriendo en estos sistemas las que deben ser interconectadas por la red. Los sistemas finales son frecuentemente dispositivos modernos, los cuales normalmente se interconectan vía LAN —típicamente clientes (estaciones de trabajo) y servidores basados en la tecnología de computadoras personales. Sin embargo, la red también tiene que soportar dispositivos de tecnología antigua —sistemas finales heredados— y estos son interconectados por lo general usando interfaces seriales. Ejemplos de esto pueden ser terminales tontas.

- *Usuarios remotos.* Se está convirtiendo cada vez más importante para los usuarios que necesitan la flexibilidad de acceso a las mismas aplicaciones de computadora como si estuvieran en su lugar de trabajo. El diseñador de red tiene el reto de acomodar un número creciente de usuarios conectándose a través de acceso vía módem.

El tipo y número de las características mencionadas son usualmente localizadas en la declaración de los requerimientos. La tarea del diseñador es desarrollar una red preparada para interconectarlos de tal forma que entreguen las aplicaciones requeridas. Para lograr esto, hay un conjunto de piezas disponibles para el diseñador:

- *Red de área local.* Consiste del cableado en sitio, usado para interconectar los sistemas finales modernos. El diseñador estará interesado en seleccionar las topologías y arquitecturas apropiadas para cada sitio.

- *Red de área amplia.* Requerida para interconectar los sitios. En esta etapa, se seleccionará la topología y tecnología para la red.

- *Red de respaldo.* Esta es una característica opcional, y será requerida en redes de misión crítica donde la WAN principal no es capaz de proveer el nivel requerido de disponibilidad al momento de hacer reparaciones.

- *Circuitos de acceso y respaldo.* Conecta los sitios a la WAN, y como tal, son normalmente una parte integral de los servicios WAN. El diseñador deberá seleccionar la velocidad de transmisión óptima para estos circuitos.

- *Dispositivo de salida WAN.* Este dispositivo es utilizado para adaptar los protocolos e interfaces utilizadas en sitio a los de la WAN. El diseñador tendrá que seleccionar la tecnología apropiada para este dispositivo, dependiendo del tipo de red local y amplia seleccionado, y los protocolos de comunicación empleados en los sistemas finales. El dispositivo de salida es comúnmente usado para servir a los equipos heredados tan bien como a los de la red moderna.

Cada uno de estos puntos necesita ser considerado en el diseño ya que todos juegan un papel en la red de alto desempeño.

3.2. Diseño LAN y LsLAN

3.2.1. Diseño LAN

El crecimiento de las LAN ha sido propiciado por la introducción de nuevas tecnologías y por la disponibilidad de computadoras personales y estaciones de trabajo robustas y asequibles. Como resultado, aplicaciones que antes solo eran posibles en grandes computadoras centralizadas ahora están corriendo en LAN. La velocidad en la red y la disponibilidad son requerimientos críticos, dictados por las aplicaciones existentes y una nueva generación de productos multimedia, de trabajo en grupo, de imagen y bases de datos que pueden fácilmente saturar una red corriendo las velocidades tradicionales. Con más aplicaciones requiriendo velocidades LAN más rápidas para un rendimiento aceptable, los administradores de red enfrentan serias opciones para implementar una tecnología LAN de alta velocidad

Las LAN pueden ser comprendidas comenzando con las topologías básicas. Todas las topologías parten del concepto básico de que todos los sistemas finales conectados a la LAN están compartiendo un medio de comunicación común. Esto no solo permite una comunicación simple entre dispositivos, también permite a un sistema final comunicarse al mismo tiempo con todos los otros sistemas conectados —característica que es ampliamente explotada en los protocolos LAN.

Las principales características que determinan la naturaleza de una red son:

- Topología.
- Medio de transmisión.
- Técnica de acceso a la medio.

Juntas determinan en gran medida el tipo de datos que pueden ser transmitidos, la velocidad y eficiencia de las comunicaciones y las clases de aplicaciones que la red puede soportar.

La topología se refiere a la forma en la cual los puntos terminales o estaciones están interconectados. Está definida por la distribución de los enlaces de comunicación y los elementos de conmutación, y determina las rutas que pueden ser usadas entre cualquier par de estaciones. Es importante notar la diferencia entre una red de comunicación y conectar directamente cualquier par de dispositivos. En la conexión punto a punto, cada dispositivo tiene un enlace directo con cada uno de los demás dispositivos. Esta configuración incrementa el costo del sistema en cuanto a la instalación del cableado y el hardware I/O conforme se agregan dispositivos. La solución es introducir una red de nodos conmutados con habilidad para dirigir los mensajes, creando enlaces lógicos y eliminando la necesidad de muchas conexiones físicas directas.

Las topologías más utilizadas para construir redes son: estrella, bus y anillo. A su vez, éstas pueden ser utilizadas como parte de otra red que utilice topologías más complejas o mezcla de ellas.

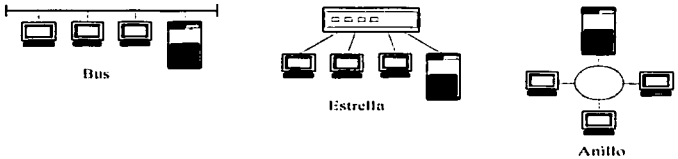


Figura 6. Topologías mas empleadas para construir redes

Los factores que se deben considerar al analizar y elegir una topología son:

- Flexibilidad para agregar y/o eliminar nodos.
- Repercusiones de alguna falla sobre algún nodo.
- Protocolo de comunicación física.
- Problemas en el flujo de la información.
- Versatilidad en el diseño del cableado.
- Probabilidad de crecimiento.
- Costo/beneficio.

Anillo

Consiste en un conjunto de repetidores unidos por enlaces punto a punto en donde el primero está conectado al último, de tal forma que cada repetidor participa en dos conexiones. El repetidor es un dispositivo capaz de recibir datos y transmitirlos bit por bit a otra conexión tan rápido como los recibe sin almacenarlos. Los enlaces son unidireccionales (los datos son transmitidos en una sola dirección) y cada estación se une a la red por medio de un repetidor. Los datos son transmitidos en paquetes. Así por ejemplo, si la estación X desea transmitir un mensaje a la estación Y, ésta descompone el mensaje en paquetes. Cada paquete contiene una porción de los datos más información de control incluyendo la dirección de la estación Y. Los paquetes son introducidos en el anillo uno a la vez y circulan hacia el otro repetidor. La estación Y reconoce su dirección y copia los paquetes como van pasando. Debido a que muchos paquetes comparten el anillo, se necesita un

control para determinar el momento en que cada estación puede insertar paquetes. El control de la red puede ser centralizado o distribuido en varios nodos.

En caso de ser centralizado, uno de los nodos actúa como controlador de forma tal que, como todos los mensajes tienen que pasar a través de él, puede verificarse el correcto funcionamiento de la red y en caso de que hubiera falla tomar las medidas necesarias para solucionarlas. Si es distribuido, el control se ejerce de manera conjunta entre varios nodos. El flujo de información estará limitado por el ancho de banda del medio de comunicación. Ya que cada estación de trabajo tiene que retransmitir cada mensaje, si existiera un número elevado de estaciones, el retardo introducido en la red puede ser muy grande para ciertas aplicaciones. Token Ring y FDDI utilizan ambas CSMA y Token Passing como métodos de acceso al medio.

Características:
- La capacidad de transmisión se reparte equitativamente entre todos los usuarios.
- Es fácil localizar los enlaces y nodos que originan errores.
- Se simplifica al máximo la distribución de mensajes.
- El tiempo de acceso no es muy grande.
- La confiabilidad de la red depende de los repetidores.
- Es necesario un dispositivo monitor.
- No es fácil incorporar nuevos dispositivos sin interrumpir la actividad de la red.

Bus

Con la topología de bus, la red de comunicación es simplemente el medio de transmisión, sin repetidores. Todas las estaciones se adhieren a través del hardware de interfase adecuado; directamente a un medio de transmisión lineal o bus. Las transmisión de cualquier estación se propaga a lo largo del medio y es recibida por todas las demás estaciones. La información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones. Por ello el protocolo mas utilizado es el CSMA/CD.

Características:
- El medio de transmisión es totalmente pasivo.
- Es fácil conectar nuevos dispositivos.
- Adecuada para tráfico muy alto.
- El sistema no reparte adecuadamente los recursos.

La red local se concentra alrededor de un coaxial grueso corriendo alrededor del edificio formando una topología de bus. El cable tiene terminadores resistivos en cada extremo (sin estos, la señales en el cable podrían ser reflejadas a lo largo del cable degradando la calidad de la señal). Este tramo de cable forma lo que se conoce como un segmento LAN. Mientras que este tipo de Ethernet no es recomendado actualmente, es importante entenderlo, ya que será comúnmente encontrado en las redes locales heredadas, y muchas de las nuevas tecnologías derivan de ésta. La tecnología 10BASE2 es una variante más reciente, utiliza un coaxial delgado menos caro, y explota los conectores BNC.

Estrella

Cada estación está conectada a un dispositivo central por medio de dos conexiones punto a punto, uno para la transmisión en cada dirección. La transmisión desde cualquier estación llega al nodo central y es retransmitida a todos los demás enlaces que salen de él. De esta manera, aunque la disposición física sea una estrella, lógicamente es un bus. Lo usual es que el nodo central ejerza todas las tareas de control y posea todos los recursos de la red.

Esta configuración presenta flexibilidad para incrementar o disminuir el número de estaciones, ya que las modificaciones necesarias no representan ninguna alteración de la estructura. Si se presentara una falla en alguna estación, la repercusión en el comportamiento de la red es muy baja, en cambio si se presentará la falla en el nodo central, se produciría un problema muy grande al afectar a toda la red.

El flujo de información puede ser elevado y los retardos introducidos por la red son pequeños debido a que la mayor parte de ese flujo ocurre entre el nodo central y los nodos periféricos.

Características:
- Ideal para configuraciones en las que hay que conectar muchas estaciones.
- Las estaciones pueden tener velocidades diferentes dependiendo del medio de transmisión.
- Se puede obtener un alto nivel de seguridad.
- Es fácil localizar las fallas.
- Es susceptible a averías en el nodo central.

3.2.2. Tecnologías de transporte

En lo que respecta a las tecnologías de transporte, para la mayoría de las aplicaciones basadas en LAN, el diseñador puede escoger entre cuatro estándares: IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), FDDI o ATM.

Ethernet generalmente provee los adaptadores de red de menor costo para los sistemas finales (y de hecho muchos sistemas finales incluyen interfaces Ethernet de fábrica). Puede proveer 10/100Mbps o 1Gbps de velocidad de transmisión, sin embargo, debido al mecanismo de colisiones usado para acceder al medio, esta capacidad no se alcanza fácilmente. La cantidad exacta va a ser una función compleja del número de sistemas finales conectados al segmento LAN, su tráfico y el tamaño de los mensajes que envíen.

Los usuarios que requieran un mayor rendimiento (por ejemplo, aquellos con intensas aplicaciones multimedia) pueden considerar el uso del estándar Ethernet a 100Mbps (100BASE-T). Servidores de alta velocidad y sistemas de usuario pueden estar conectados usando el estándar Gigabit Ethernet. Para organizaciones con instalaciones Ethernet existentes, incrementar la velocidad de la red a 100Mbps es preferible a invertir en una tecnología LAN completamente nueva.

Token Ring es ampliamente utilizado, aunque no exclusivo, en ambientes IBM. Las instalaciones pueden ser diseñadas para operar hasta 16Mbps. El método token passing de acceso al medio de este tipo de LAN asegura que la utilización pueda alcanzar el 100%, dando un rendimiento mayor que Ethernet. Token Ring también puede tener mejores capacidades de administración que Ethernet (ya que siempre hay tráfico token circulando, éste puede ser monitoreado, y la falla puede ser rápidamente detectada). La tecnología Token Ring también permite el diseño de respaldos en diseños LAN a gran escala con Ethernet. El punto en contra de Token Ring es el costo elevado del equipo asociado.

FDDI es una importante tecnología basada en una estructura dual de fibra óptica, diseñado para ser usado a gran escala y proveer el backbone para interconectar redes locales en diferentes pisos o edificios a través de un cámpus. Alcanza altas velocidades (100Mbps), distancias largas entre estaciones y una alta confiabilidad (debido a su estructura de doble anillo). Es una tecnología comparativamente cara, y normalmente no es utilizada directamente en sistemas finales, a menos que requieran específicamente el gran ancho de banda y la redundancia que ofrece. Esta tecnología ha comenzado a desaparecer a pesar de sus ventajas, reemplazada por las redes Ethernet de fibra óptica y la tecnología ATM.

ATM comenzó su vida como una tecnología WAN, pero ha sido adoptada para utilizarse en redes locales. Es posible diseñar ATM al escritorio (utilizando por lo general interfaces ATM de 25Mbps), aunque no es conveniente pues resulta más caro que Ethernet a 100Mbps. ATM generalmente encuentra su lugar en el backbone de grandes cámpus, es orientado a conexión, punto a punto, full duplex y utiliza un pequeño y fijo tamaño de paquete llamado "celda". Las aplicaciones que necesiten comunicarse a través de una LAN ATM primero deben establecer una VC (Virtual Connection). La VC es un camino a través del cual uno o más switches proveen una tubería punta a punta para transportar la información. Las VC's son establecidas en dos pasos. Primero, un PVC (Permanent Virtual Circuit) que puede ser manualmente configurado por el administrador de red. Segundo, un SVC (Switched Virtual Circuit) que es establecido en el proceso de llamado en el momento que se necesite. ATM a 155Mbps es una topología de malla, lo cual significa que un equipo en la red puede ser alcanzado desde cualquier otro punto usando múltiples rutas.

Cada una de las arquitecturas presentadas probablemente conecten otro tipo de LAN o backbone. Algunas propiedades importantes para los backbone de alta velocidad son: la distancia punto a punto, la robustez y disponibilidad de la tecnología y el costo incremental por conectar grupos de trabajo al backbone.

3.2.2.1. Ethernet

El término Ethernet se refiere a la familia de implementaciones LAN que incluyen tres categorías principales:

- *Ethernet*. Especificaciones LAN que operan a 10Mbps sobre cable coaxial.
- *Ethernet 100Mbps*. Especificación también conocida como Fast Ethernet que opera a 100Mbps sobre cable de fibra óptica y par trenzado.
- *Ethernet 1000Mbps*. Especificación también conocida como Gigabit Ethernet que opera a 1000Mbps (1Gbps) sobre cable de fibra óptica y par trenzado.

Por su parte IEEE creó estandares para cada una de ellas comprendidos en el estandar 802.3, éste proporciona una variedad de opciones de cableado incluyendo 10Base5, 10Base2, 10BaseT, 10BaseFL y 100BaseT.

Ethernet

Ethernet es una especificación LAN que opera a 10Mbps usando CSMA/CD (Carrier Sense Multiple Access Collision Detection) para correr sobre cable coaxial grueso. Ethernet fue diseñado para servir en redes con altos requerimientos ocasionales y esporádicos de tráfico, y la especificación IEEE 802.3 fue diseñada basada en la tecnología Ethernet original.

Ethernet es usualmente implementado en tarjetas de red o circuitos impresos. Las convenciones de cableado para Ethernet especifican el uso de un transceiver para conectar el cable al medio físico de red. El transceiver lleva a cabo muchas de las funciones de la capa física, incluyendo la detección de colisiones. El cable del transceiver conecta las estaciones finales.

En ambientes basados en broadcast Ethernet, todas las estaciones ven todos los paquetes puestos en la red. Durante la transmisión, cada estación debe examinar cada paquete para determinar su dirección destino. Los paquetes identificados como propios a la estación son pasados a protocolos de capas superiores.

Dentro del proceso Ethernet de acceso al medio, cualquier estación en una red LAN CSMA/CD puede acceder a la red en cualquier momento. Antes de iniciar una transmisión, revisa el canal para confirmar que la red no está ocupada. La estación entonces transmite, verificando que la transmisión no haya sufrido alguna colisión (debido a que más estaciones sean agregadas, incrementen el volumen de tráfico que envían o decidan transmitir al mismo tiempo). Si no se detecta una colisión, la estación puede iniciar otra transmisión después de un cierto intervalo de tiempo. Si una colisión es detectada, la estación recalendariza la transmisión dentro de un intervalo de tiempo aleatoriamente seleccionado.

Características	Valores IEEE 802.3				
	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Mbps	10	10	10	10	100
Señalización	Banda base	Banda base	Banda base	Banda base	Banda base
Longitud max.	500	185	100	2.000	100
Medio	Coaxial grueso 50 ohms	Coaxial delgado 50 ohms	Cable par trenzado	Fibra óptica	Cable par trenzado
Topología	Bus	Bus	Estrella	Punto a punto	Estrella

Tabla 1. Comparativo entre estándares comprendidos en la IEEE 802.3

El parámetro principal dentro del protocolo de acceso al medio es el *slot-time*, el cual es el periodo de tiempo requerido por una estación para asegurar que no ha experimentado una colisión en una LAN apropiadamente configurada. Este parámetro, que determina el tamaño mínimo válido para un paquete, está enmarcado por el retraso total de la red. El paquete debe "llenar" toda la red antes de que la adquisición del canal sea asegurada.

y, si ocurre una colisión, la notificación pueda tener el tiempo para propagarse de regreso al transmisor y sea detectada antes de que termine el slot-time. Al incrementar la velocidad de transmisión por un factor de 10 sin modificar la MAC de 512 bits del slot-time se requiere que el diámetro de la red disminuya en un factor de 10.

Existen ciertas diferencias en los servicios que distinguen a los estándares comprendidos en la IEEE 802.3, mostrados en la tabla 1.

10Base-T

Las LAN 10BASE5 y 10BASE2 son difíciles de instalar (especialmente 10BASE5 con el coaxial grueso), también son poco flexibles una vez instalados, haciendo que las reorganizaciones sean muy laboriosas. El uso de un cableado tipo estrella es más fácil de planear y mucho más flexible. Un edificio puede ser cableado desde un lugar central a cualquier punto donde el usuario quiera situarse. Esto es idéntico al utilizado para cablear equipo telefónico (es una práctica común proveer múltiples cables a cada escritorio los cuales pueden ser usados para conexión telefónica o de red, terminados en un conector hembra (RJ45)).

100BaseT

100BaseT utiliza la especificación CSMA/CD existente en IEEE 802.3. Como resultado, 100BaseT mantiene el formato de la trama IEEE 802.3, tamaño y mecanismo de detección de errores. Además, soporta aplicaciones y software corriendo en redes 802.3. 100BaseT a una velocidades de 100Mbps.

100BaseT soporta dos tipos de señalización:

- *100BaseX*. Es el esquema de señalización empleado en 100BaseTX y 100BaseFX. 100BaseTX utiliza un par para transmisión y otro par para detección de colisiones y recepción, con cableado UTP y STP Cat. 5. 100BaseFX utiliza una fibra para transmisión y otra fibra para detección de colisiones y recepción, con hilos de 62.5/125 µm.

- *4T+*. Este esquema utiliza tres pares para la transmisión a 100Mbps y el cuarto par para detección de colisiones. Este método reduce la transmisión 100BaseT4 a 33Mbps por par, haciéndolo recomendable para cableado Cat. 3, 4 y 5.

Características	100BaseTX	100BaseFX	100BaseT4
Cable	UTP Cat. 5 ó STP tipo 1 y tipo 2	Fibra multimodo de 62.5/125 µm	UTP Cat. 3, 4 ó 5
No. de pares o hilos	2 pares	2 hilos	4 pares
Conector	Conector ISO 8877 (RJ45)	Conector duplex SC o ST	Conector ISO 8877 (RJ45)
Long. max. por segmento	100 metros	400 metros	100 metros

Tabla 2. Comparativo para las especificaciones comprendidas en 100BaseT

La especificación IEEE 802.3u para redes 100BaseTX permite un máximo de dos redes con repetidor (hubs) y una diámetro de 210 metros. Un segmento de red, el cual está definido como una conexión punto a punto entre dos dispositivos, puede ser de hasta 100 metros.

La especificación IEEE 802.3u para redes 100BaseFX permite enlaces entre equipos terminales (DTE) de aproximadamente 400 metros, o un repetidor de red de aproximadamente 300 metros de longitud.

La especificación IEEE 802.3u para redes 100BaseT4 permite un máximo de dos repetidores de red y una longitud total de aproximadamente 200 metros.

100VG-AnyLAN

100VG-AnyLAN fue desarrollado como una alternativa a CSMA/CD para aplicaciones sensitivas como multimedia. El método de acceso funciona bajo demanda y fué diseñado como una mejora a Ethernet y Token Ring de 16Mbps. 100VG-AnyLAN soporta los siguientes tipos de cables:

- 4 pares de UTP Cat. 3
- 2 pares de UTP Cat. 4 ó 5
- STP
- Fibra óptica

El estándar IEEE 802.12 100VG-AnyLAN especifica limitaciones en distancia, configuraciones de hubs y distancias máximas. Las distancias de un enlace entre un hub y un nodo son de 100 metros (UTP Cat. 3) o 150 metros (UTP Cat. 5).

Los hubs 100VG-AnyLAN son situados de forma jerárquica. Cada hub tiene al menos un puerto de enlace y pueden ser *cascadeados* hasta tres niveles y estar separados hasta 100 metros.

Las limitaciones de distancia para una red de punta a punta son de 600 metros (UTP Cat. 3) o 900 metros (UTP Cat. 5). Si los hubs están localizados en el mismo closet de cableado, las distancias se reducen a 200 metros (UTP Cat. 3 y UTP Cat. 5)

100VG-AnyLAN usa un método de acceso al medio bajo demanda que elimina las colisiones y puede ser más cargado que 100BaseT. El protocolo *Demand Priority* utiliza un esquema de arbitraje tipo *round-robin* de dos prioridades, el cual es controlado por un hub central, de primer nivel o raíz. Las estaciones y los hubs desprenden del nodo central en forma de árbol. El hub central pasa el control por el derecho de transmitir a cada hub, de puerto en puerto. El protocolo soporta dos tipos de peticiones de transmisión, referidas como de Prioridad Normal o Prioridad Alta (ej. aplicaciones de videoconferencia). Las peticiones con prioridad alta son atendidas por sobre las peticiones normales. Para asegurar equitatividad a todas las estaciones, un hub no otorga el acceso a un puerto más de dos veces en una ronda. Si una petición con prioridad normal ha permanecido pendiente por más 200 ó 300 ms, es promovida por el hub para una prioridad alta y atendida por la cola correspondiente.

Cada hub mantiene una tabla usada para almacenar las direcciones de las estaciones conectadas a cada puerto. Cuando un paquete es recibido, el hub almacena el paquete lo suficiente como para determinar la dirección destino y reenviar el paquete al puerto correspondiente a dicha dirección. El hub también reenvía el paquete al puerto de cascada usado para conectar al hub a un nivel más alto en el árbol, y a todos los puertos que hayan sido configurados como promiscuos al momento de la inicialización. Todos los demás puertos reciben una señal de espera, lo cual provee un importante nivel de seguridad.

Cuando una estación o hub desea unirse a la red, inicia una secuencia de entrenamiento consistente de un intercambio de tramas entre él mismo y el puerto al cual se conecta. Este periodo de entrenamiento dura entre 2 a 5 ms. Durante el entrenamiento, la red suspende la operación round-robin.

Las estaciones y hubs envían una señal de espera para indicar a los demás que el canal esta disponible para transmitir. La estación que desee transmitir envía una petición de transmisión al hub, indicando la prioridad. Después espera la respuesta que le permita enviar un paquete a través de la red. Si hay una petición con prioridad alta en cualquier parte de la red, el control pasa al hub solicitante y se regresa al hub original cuando la petición con prioridad alta haya terminado.

Gigabit Ethernet

Gigabit Ethernet es una extensión del estándar Ethernet IEEE 802.3. Se basa en el protocolo Ethernet pero incrementa la velocidad en un factor de 10 hasta 1000Mbps. Para acelerar la velocidad de 100Mbps a 1Gpbs, se han hecho cambios en la interfaz física al mismo tiempo que se ha mantenido idéntico para la capa de enlace.

La especificación Gigabit Ethernet IEEE 802.3z establece tres métodos para la transmisión: Laser LW (Long-Wave) sobre fibra óptica multimodo y monomodo (conocido como 1000BaseLX), laser SW (Short-Wave) sobre fibra óptica multimodo (conocido como 1000BaseSX) y el medio 1000BaseCX que permite la transmisión sobre cable blindado de par trenzado de 150 ohms balanceado. El estándar IEEE 802.3ab también especifica el uso de cable UTP para la transmisión de Gigabit Ethernet (1000BaseT) permitiendo una distancia de hasta 100 metros sobre cable Cat. 5e en adelante.

La principal diferencia entre el uso de las técnicas LX o SX son el costo y la distancia. Los láser SX cuestan menos, pero se desempeñan a una distancia más corta. En contraste, los láser LX son más caros pero logran mayores distancias.

Para corridas de cable más cortas (25 metros o menos), Gigabit Ethernet permite la transmisión sobre cable blindado de 150 ohms balanceado. Con el propósito de incrementar la seguridad y reducir la interferencia causadas por fenómenos externos y diferencias de voltaje, los transmisores y receptores comparten una tierra en común.

Para la transmisión half duplex, CSMA/CD debe ser usado para asegurar que las estaciones puedan comunicarse y que la recuperación de colisiones pueda llevarse a cabo. Debido a que CSMA/CD es sensitivo al retraso, deben tomarse ciertas consideraciones. Un dominio de colisión está definido como el tiempo de transmisión de una trama valida. Esta transmisión dicta la separación máxima entre dos estaciones en un segmento compartido. Conforme se incrementa la velocidad de operación, el tiempo mínimo de transmisión para una trama decrementa, así como el dominio de colisiones. Aumentar la velocidad de Ethernet a Gigabit crea algunos retos en la implementación de CSMA/CD. Como se explicó anteriormente, a velocidades mayores a 100Mbps, los paquetes de tamaño más pequeño son más pequeños que la longitud de *slot-time* en bits (slot-time es definido como la unidad de tiempo de Ethernet MAC para manejar una colisión). Para remediar este problema, se agregan extensiones a la especificación Ethernet hasta que la trama cumpla con el mínimo *slot-time* requerido. De esta forma, los paquetes de menor tamaño pueden coincidir con el mínimo *slot-time* y permitir una operación controlada con CSMA/CD. Otro cambio a la especificación Ethernet es la adición de tramas de relleno. Estas tramas son una característica opcional en la cual una estación final puede transmitir tramas de relleno sobre el cable para no tener que renunciar a la transmisión. Las demás estaciones posponen su transmisión mientras no haya inactividad en el cable.

3.2.2.2. FDDI

FDDI (Fiber Distributed Data Interfase) especifica un token-passing de 100Mbps sobre una LAN de doble anillo usando cable de fibra óptica. FDDI es frecuentemente usado como una tecnología de backbone de alta velocidad debido a su soporte para altos anchos de banda y mayores distancias que el cobre. También existe la especificación llamada CDDI (Copper Distributed Data Interfase) que ha surgido para proveer servicio a 100Mbps sobre cobre. CDDI es la implementación de los protocolos FDDI sobre cable par trenzado.

FDDI utiliza una arquitectura de anillo dual con tráfico en cada anillo fluyendo en direcciones opuestas. Los anillos duales consisten de un anillo primario y otro secundario. Durante la operación normal, el anillo primario es usado para la transmisión de información y el segundo se mantiene en espera. El objetivo principal de los anillos duales es proveer una confiabilidad y robustez superior. La figura 7 muestra el anillo primario (en sentido de las manecillas del reloj) y el secundario.

FDDI fué desarrollado por el comité de estándares ANSI (American National Standards Institute) a mediados de los 80's. En ese tiempo, las estaciones de trabajo de alta velocidad comenzaron a demandar más recursos de las redes locales existentes basadas en Ethernet y Token Ring. Al mismo tiempo, la confiabilidad en la red se había convertido en un aspecto cada vez más importante conforme los administradores de sistemas migraron aplicaciones de misión crítica de grandes computadoras hacia la red. FDDI llegó para resolver estas necesidades.

FDDI utiliza fibra óptica como el medio de transmisión principal, pero también puede correr sobre cable de cobre. Como se mencionó anteriormente, FDDI sobre cobre se conoce como CDDI. La fibra óptica tiene

varias ventajas sobre el cobre. En particular, la seguridad, confiabilidad y el rendimiento son incrementados con la fibra óptica ya que ésta no emite señales eléctricas. Un medio físico que emite señales eléctricas (cobre) puede ser "puenteado" y en consecuencia permitir accesos no autorizados a la información que está transitando en el medio. Además, la fibra es inmune a la interferencia eléctrica de tipo RFI (Radio Frecuency Interference) y EMI (Electromagnetic Interference).

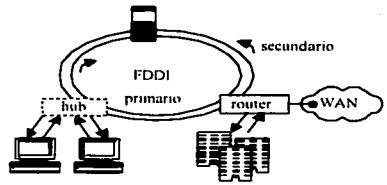


Figura 7. Arquitectura empleada en FDDI funcionando con dos anillos

FDDI define dos tipos de fibra óptica: monomodo y multimodo. Un modo es un rayo de luz que entra en la fibra en un ángulo particular. La fibra multimodo utiliza un LED como dispositivo generador de luz , mientras que la fibra monomodo generalmente utiliza láser. La fibra multimodo permite múltiples modos para que la luz se propague a través de ella. Debido a que solo es usado un modo en la fibra monomodo, ésta es capaz de entregar un mayor rendimiento sobre distancias más grandes, por lo cual es usada para la conectividad entre ambientes que están geográficamente más dispersos.

Una de las características únicas de FDDI es que existen múltiples formas de conectar dispositivos. FDDI define tres tipos de dispositivos: SAS (Single-Attachement Station), DAS (Dual-Attachement Station) y un hub. Un SAS se conecta solo a un anillo (el primario) a través del hub. Una de las ventajas principales de conectar dispositivos de tipo SAS es que estos no van a tener efecto alguno en el anillo si son desconectados o apagados.

Cada DAS FDDI tiene dos puertos, designados A y B. Éstos puertos conectan al DAS al anillo dual FDDI. Por lo tanto, cada puerto provee una conexión para cada anillo. Los dispositivos DAS pueden afectar el anillo si son desconectados o apagados.

Un hub FDDI (también llamado DAC, Dual-Attachement Concentrator) es el bloque de construcción de una red FDDI. Se conecta directamente a ambos anillos lo que asegura que las fallas o desconexiones de cualquier SAS no afecten en el anillo. Esto es particularmente útil cuando PC's o dispositivos similares que constantemente se encienden o apagan se conectan al anillo. La figura 8 muestra éstas características.

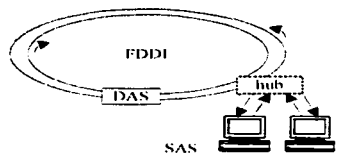
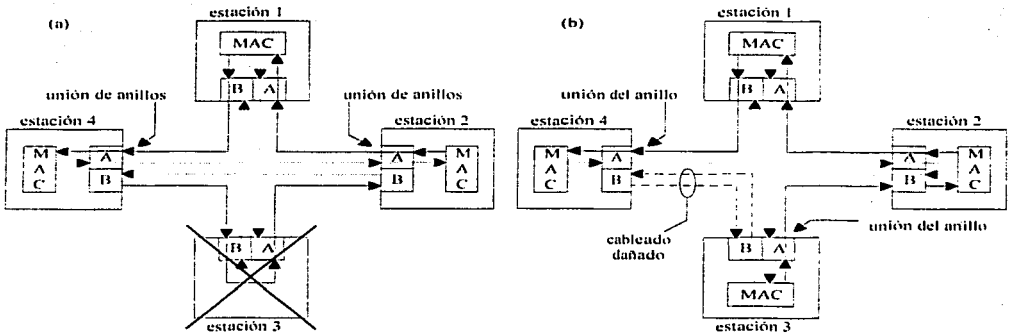


Figura 8. Dispositivos de conexión utilizados en FDDI

FDDI provee un cierto número de características de tolerancia a fallas:

- *Doble anillo.* Si una estación en el doble anillo falla o es apagada, o si el cable es dañado, el anillo dual es automáticamente bloqueado, con lo que se vuelve una topología de un solo anillo. La información continúa siendo transmitida en el anillo FDDI sin impactar en el rendimiento durante estas condiciones. Las figuras 9.a y 9.b ilustran el efecto de un anillo configurado de ésta manera.



Figuras 9.a y 9.b. Tolerancia a fallas basándose en el doble anillo de FDDI

Cuando una sola estación falla, como es mostrado en el figura 9.a, los dispositivos a cada lado se bloquean formando un solo anillo y la operación de la red continúa para las estaciones restantes en el anillo. Cuando ocurre una falla en el cable, como se muestra en la figura 9.b, los dispositivos a cada lado modifican su conexión permitiendo que el servicio continúe para todas las estaciones. Debe notarse que FDDI verdaderamente provee tolerancia contra una sola falla. Cuando dos o más fallas ocurren, FDDI bloquea los anillos en dos o más anillos independientes, haciéndolos incapaces de comunicarse entre ellos.

- *Switch bypass.* Provee operación continua en el anillo dual si un dispositivo falla. Es usado para proporcionar la segmentación del anillo y eliminar las estaciones con fallas del anillo.

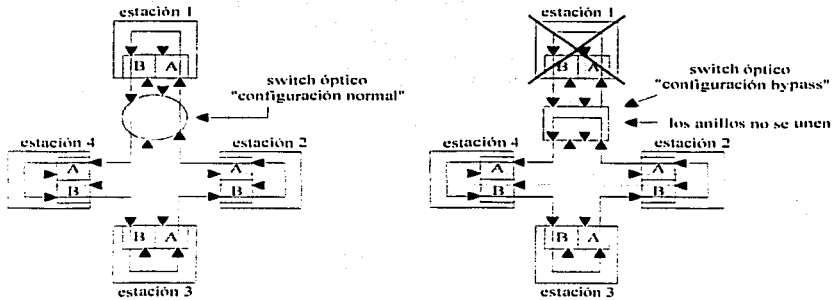


Figura 10. Tolerancia a fallas basándose en el switch bypass de FDDI

Este tipo de switch realiza sus funciones a través del uso de espejos ópticos que pasan la luz del anillo directamente al dispositivo DAS durante la operación normal. En el caso de una falla en el dispositivo DAS, como una falla de energía, el switch va a pasar la luz a través de él mismo usando los espejos internos y manteniendo la integridad del anillo. El beneficio de ésta característica es que el anillo no va a entrar en bloqueo en caso de que un dispositivo falle. La figura 10 muestra la funcionalidad del switch bypass.

- *Dual homming*
  Los dispositivos críticos, como routers o estaciones de trabajo, pueden utilizar una técnica de tolerancia a fallas llamada *dual homming* para proveer redundancia adicional y ayudar a garantizar su operación. En una configuración dual homming, los dispositivos críticos son conectados a dos hubs. La figura 11 muestra una configuración para dispositivos tales como servidores de archivos y routers.

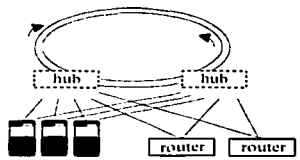


Figura 11. Tolerancia a fallas basándose en el dual homming de FDDI

Un par de enlaces es declarado como enlace activo; el otro par es declarado pasivo. El enlace pasivo está en modo de respaldo hasta que el enlace primario tenga una falla. Cuando esto ocurre, el enlace pasivo automáticamente cambia de estado.

El protocolo MAC provee una inicialización del anillo y dos categorías de servicio (prioridades) llamadas, asíncrono y síncrono. Cada estación puede usar una o ambas. La primera es el servicio síncrono. La estación tiene permitido capturar el token cada vez que pase por ella y originar un número de paquetes relacionados. Esto permite al administrador de red otorgar prioridad a ciertas estaciones y provee una latencia mínima. El servicio asíncrono divide la capacidad no consumida por las estaciones síncronas entre todas las estaciones por igual.

En resumen, las tablas 3.a, 3.b y 3.c son un compendio de los parámetros relevantes de los cuatro protocolos y los puntos expuestos. Como podrá observarse, no se listan las características de Ethernet a 10Mbps o Token Ring a 4/16Mbps por considerar que ya existen tecnologías que representan la evolución, o han partido, de ellas. Tampoco hay una sección que trate ATM con un poco más de detalle, y esto es debido a que aún no se ha definido en su totalidad, se necesitan protocolos que integren ATM con otras redes (sobre todo las heredadas), existe una gran base instalada en Ethernet y el usuario promedio va a preferir actualizar en lugar de realizar un cambio completo y representar un costo mayor. Sin embargo, dado que ya existen redes instaladas y operando, se agrega a la tablas con sus características.

Características

	FDDI	100BaseT	VG-AnyLAN	ATM
# estaciones	500	1024	-----	implementación
Método de acceso	Token passing	CSMA/CD	Round Robin	Full duplex
Tamaño de paquete	4500 bytes	1500 bytes	1500 ó 4500	Celda 48 byte
Diámetro	100km	210km	2.5km	-----
Complejidad	Media	Baja	Media	Alta

Tabla 3.a. Características físicas relevantes a cada tecnología de transporte

Topología

	FDDI	100BaseT	VG-AnyLAN	ATM
Topología	Anillo dual con árbol	Estrella	Estrella jerárquica	Malla
UTP Cat. 5	100m	100m	100m	100m
STP 150 ohms	100m	100m	100m	100m
Fibra multimodo	2km	-----	500m (805nm)	2km
Fibra monomodo	60km	-----	2k (1300nm)	40km

Tabla 3.b. Medios de transmisión establecidos para cada tecnología de transporte

Eficiencia

Tamaño paquete (bytes)	VG-AnyLAN 1 hub, 200m	VG-AnyLAN 3 hubs, 2.2km	100BaseT 210m	FDDI 3 hubs, 2.2km	ATM 1 enlace
64	46%	19%	65%	84%	58%
128	63%	32%	74%	91%	78%
256	77%	49%	80%	96%	78%
512	87%	66%	83%	98%	85%
1024	93%	79%	86%	99%	85%
1518	95%	85%	87%	99%	86%

Tabla 3.c. Eficiencia estimada para cada tecnología de transporte

La tercera tabla merece un poco de explicación. Para facilitar su entendimiento, vamos a tomar la siguiente configuración de ejemplo. El ancho de banda disponible para un usuario es la velocidad de transmisión menos la eficiencia, rango en el cual la LAN es saturada y la carga adicional no puede ser transportada. Debido a las diferencias entre los protocolos, la comparación es un poco difícil. La configuración provee estaciones a la máxima separación para el análisis de un peor caso, pero las distancias límite en los protocolos difieren. El análisis incluye VG-AnyLAN para dos distancias basadas en la extensión física —un tamaño moderadamente largo y otro corto, coincidente con el máximo para 100BaseT. FDDI tiene una distancia similar a VG-AnyLAN para efectos de comparación. ATM es configurado como un solo enlace entre un switch y una estación. Las características físicas son:

	VG-AnyLAN		100BaseT	FDDI	ATM
# estaciones	20	20	20	20	1
# hubs	1	3	2	3	1
Diámetro	200m	2.2km	210m	2.2km	-----

Tabla 2. Características físicas propuestas para ejemplificar la eficiencia

La configuración VG-AnyLAN con mayor distancia, también es usada para FDDI, mostrada en la figura 12.a; tres hubs con uno como raíz, y conectados por cables duplex a 1km. Las estaciones son conectadas a los hubs inferiores usando cables duplex de 100m. El diámetro total es igual y dispuesto a 2.2km.

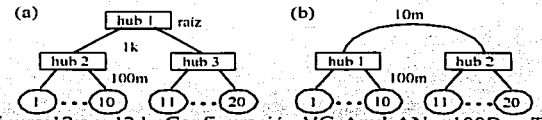


Figura 12.a y 12.b. Configuración VG-AnyLAN y 100BaseT, respectivamente, empleando la mayor distancia

La topología 100BaseT mostrada en la figura 12.b, contiene dos hubs, cada uno con estaciones conectadas con cables duplex a 100m. Los dos hubs tienen un cable de 10m conectándolos.

A continuación se expondrán los detalles del modelo, utilizando VG-AnyLAN como ejemplo. En caso de que el lector requiera más detalle sobre los cuatro protocolos tendrá que realizar un estudio más a conciencia refiriéndose a la documentación correspondiente.

La eficiencia del protocolo es simplemente el tiempo en transmitir una trama, F, dividida entre F más el overhead (OH) asociado a la transmisión:

E = eficiencia = F / (F + OH)

El modelo toma en cuenta el overhead creado por el procesamiento del hub sobre las peticiones para transmitir, la operación para conocer las direcciones, los pasos para arbitrar realizados por el hub raíz y el retraso en la propagación a través del medio.

Una estación debe solicitar acceso para transmitir paquetes y recibir un *acknowledge* (notificación de recibido). El tiempo para este proceso en un solo hub incluye el tiempo necesario para que el hub procese la petición (t_req) más el tiempo para procesar el acknowledge en el hub solicitante (t_grant):

t_ack = t_req + t_grant

El tiempo t_ack en el caso de cascada en simplemente L veces el valor de un solo hub, donde L es el número de niveles de hubs:

t_ack_mult = L * t_ack

De la definición del estándar se han escogido cuidadosamente valores razonables para t_req y t_grant, siendo de 1.5 microsegundos cada uno.

La siguiente contribución al overhead es el tiempo requerido por el hub para reconocer la dirección destino en el paquete. Durante este proceso el hub almacena el paquete. Este overhead, t_adrs, es seleccionado basado en el hecho de que se necesitan recibir aproximadamente 14 bytes para resolver, del cual se espera un total de 1.2 microsegundos.

El overhead total originado por la revisión de direcciones en los hubs es un poco más complejo: la revisión de la dirección tiene que progresar L niveles hacia arriba en la cascada hacia el hub raíz, y después tiene que regresar hasta el hub destino antes de llegar a la estación solicitada. Por lo tanto, los paquetes individuales incurren en el almacenamiento a 2L-1 hubs (L hubs hacia arriba y (L-1) hubs de regreso):

t_adrs_mult = (L * t-adrs) + (L-1 * t_adrs)

El retraso en la propagación es el retraso total en el camino físico que sigue un paquete hacia el hub raíz y de regreso a la estación transmisora. Por ejemplo, 2.2km de medio a 5uS/Km. contribuyen a un retraso, t_prop, de 11 microsegundos.

La eficiencia también involucra el tiempo en transmitir un paquete:

F = (tamaño de paquete en bytes) * 80nS/byte

y el formato de cabecera para la trama (8 bytes de preámbulo y 2 bytes de limitador):

Tped = (10 bytes) * 80nS/byte

Por lo tanto,

E = F / (F + Tped + t_ack_mult + t_adrs_mult + t_prop)

Los resultados son presentados en la tabla anterior y se pueden obtener dos conclusiones. Primero, puede ser visto que la eficiencia de VG-AnyLAN es similar a 100BaseT en la configuración pequeña. 100BaseT tiene una eficiencia mayor a 77% para paquetes de tamaño regular (256 bytes), lo cual es aceptable. Segundo, los resultados para el caso de tres hubs muestran que la cascada tiene un impacto significativo con los paquetes de tamaño pequeño.

3.2.3. Diseño LsLAN

La limitación clave con los diseños LAN descritos en las secciones previas es el ancho de banda. Los diseños descritos operan como un único y compartido medio físico y sólo una estación en la LAN es capaz de transmitir a la vez. Entre más estaciones en la LAN, menor es el ancho de banda disponible para cada una.

Otra limitación clave en estas LAN es la distancia. Con Ethernet, la distancia no debe ser muy larga, ya que el mecanismo de colisión no opera correctamente. Con FDDI, el retardo de las tramas propagándose alrededor del anillo puede volverse excesivo. Los diseños LAN a gran escala deben superar estas limitaciones.

3.2.3.1. Bridges Ethernet

Una típica red con bridges es mostrada en la figura 13.

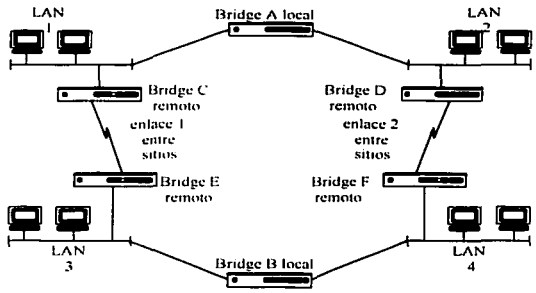


Figura 13. Ejemplo de una red empleando bridges

Se muestran dos tipos de bridges: el bridge local (usado para enlazar dos LAN en el mismo sitio) y el bridge remoto (usado para enlazar dos sitios).

Estos dispositivos son generalmente fáciles de usar, ya que son autoconfigurables. Imagine que el bridge A acaba de ser instalado. Va a recibir paquetes de la LAN1, pasarlos a la LAN2 y viceversa. Conforme pasa paquetes, observa la dirección MAC origen y graba esto contra el puerto por el cual el paquete entró al bridge. En el futuro, cuando la LAN vea un paquete con esa dirección MAC destino, sabrá en que puerto está conectada. Esto significa que si un paquete tiene un origen en LAN1 y está destinado a una dirección MAC encontrada en LAN1, el bridge no necesita reenviarlo a LAN2. Conforme el bridge aprende donde está cada dirección MAC en la red, reenvía menos y menos paquetes. Esto tiene dos ventajas claras:

- A pesar de un diseño usando repetidores, el tráfico local a un segmento LAN se mantiene local. Esto reduce tráfico en otros segmentos LAN.
- En el caso de repetidores remotos, el ancho de banda disponible en el enlace debe ser utilizado enviando sólo el tráfico necesario para mejorar el uso del ancho de banda disponible.

Así como trabajan en modo de auto-aprendizaje, los bridges son capaces de ser configurados con información estática de MAC's. Esto puede ser una característica útil de seguridad, ya que se puede limitar a los usuarios que tienen permitido comunicarse a través de los bridges.

En diseños de bridges, es importante notar que los paquetes de broadcast son siempre enviados a través de los bridges. Esto significa que en el diseño de la figura 13, estos paquetes de broadcast pueden reenviarse indefinidamente alrededor de los bridges (ej. loop). Para prevenir esto, los bridges utilizan un protocolo llamado Spanning Tree. Los bridges envían sus propios mensajes orientados a identificar otros bridges. Se comunican entre sí para establecer la topología de la red. Después reducirán la red desconectando los enlaces redundantes entre ellos, para que siempre haya un solo camino entre dos puntos. El protocolo requiere que los bridges se comuniquen cada 2 segundos y esto utiliza una cantidad considerable de ancho de banda. Por otro lado, una conexión de red inestable es rápidamente descubierta y la red puede reconfigurarse activando los

enlaces previamente desconectados. Esto significa que el diseño tiene una buena redundancia contra las fallas en los enlaces o en los bridges.

Una característica útil en los bridges es que son capaces de interconectar diferentes tipos de adaptadores LAN, por ejemplo, LAN1 puede ser 10BASET y LAN2 puede ser 100BASET. Los bridges capaces de manejar diferentes velocidades son generalmente capaces de sensar automáticamente la velocidad de la LAN y autoconfigurarse.

3.2.3.2. Switches

Los switches LAN son efectivamente bridges multipuerto. Son configurados (o aprenden) con la lista de direcciones MAC conectadas a cada puerto. En un ambiente switcheado, el tráfico LAN está presente solamente en segmentos LAN conteniendo las direcciones origen y destino, liberando ancho de banda en otras LAN para ser usado por otros usuarios.

Los switches LAN existen en una variedad de tamaños. Las típicas unidades finales soportaran 8/12/24 puertos hasta las unidades de gran capacidad manejando probablemente 100 puertos. Pueden ser usados en el mismo lugar que un hub en el diseño de red —de hecho actualizar un hub a switch es una práctica común para mejorar el rendimiento de la red.

El precio de los switches LAN tiende a ser mayor por puerto que un hub, así que puede no ser costeable usar un switch en todos los lugares. En estos casos, el switch es generalmente instalado como un dispositivo de backbone, con puertos conectados a hubs, los cuales a su vez sirven a grupos de usuarios finales. En lo posible, uno asegura que los grupos de usuarios que se comunican entre ellos estén localizados en el mismo segmento LAN, junto con los servidores específicos para ese grupo de trabajo. Cuando los usuarios miembros de un mismo grupo de trabajo se encuentran ubicados en diferentes segmentos LAN, es posible emplear VLAN para interconectarlos de forma lógica, como si estuvieran situados físicamente en el mismo lugar. Como en el caso de los bridges, el Spanning Tree es utilizado para evitar loops.

Cuando se utilizan VLAN, existe generalmente la necesidad de que fluya algo de tráfico entre VLAN (ej. un servidor compartido). Un router es usado para encaminar el tráfico entre VLAN. Los routers pueden ser equipos con filtros sofisticados para determinar que tráfico está permitido que fluya entre VLAN.

El router conectado al switch debe ser capaz de identificar la membresía de la VLAN para cada trama. Los switches de mayor tamaño son modulares en su diseño, y pueden usualmente acomodar una tarjeta de ruteo para llevar a cabo estas funciones.

3.2.4. Diseño de topología WAN

Un factor clave para decidir que tipo de tecnología de área amplia instalar será la topología de la red. Esto puede ser entendido como la forma general de la red, o que sitio está conectado con cual. Note que es importante saber cuales sitios necesitan comunicarse. Es razonable esperar que aquellos sitios que intercambien el volumen de información más grande sean conectados directamente. Sin embargo, puede no ser costeable interconectar todos los sitios que necesiten comunicarse. Aquellos con intercambio de cantidades pequeñas de información pueden ser enlazados a través de sitios de transito intermedio. Las topologías son mostradas en la figura 14.

1 a 1 — punto-a-punto

Este es el caso más simple, con un sitio comunicándose con otro. En la red de alto desempeño, usualmente hay dos sitios clave en cada extremo.

Muchos a 1 — estrella o centralizada

Es una forma extendida de punto-a-punto, con muchos circuitos punto-a-punto individuales convergiendo a un sitio central. Un ejemplo puede ser un nodo principal con conexión hacia nodos secundarios de

interconexión. La mayoría del tráfico fluirá entre los nodos secundarios y el principal. En esta topología, si los secundarios necesitan comunicarse con otro, sólo pueden hacerlo a través del sitio central.

Muchos a 2 — centralizada dual

Es una extensión especial de la topología muchos a 1, la cual vale la pena mencionarla, simplemente porque es muy común. Es usada típicamente cuando hay dos sitios principales. Los dos sitios proveen redundancia, ya que la aplicación puede ser satisfactoriamente ejecutada usando solamente un sitio (bajo circunstancias normales, ambos sitios pueden compartir el tráfico, o permanecer en modo de espera únicamente). Los nodos secundarios van a necesitar una conexión a ambos sitios para obtener redundancia contra fallas.

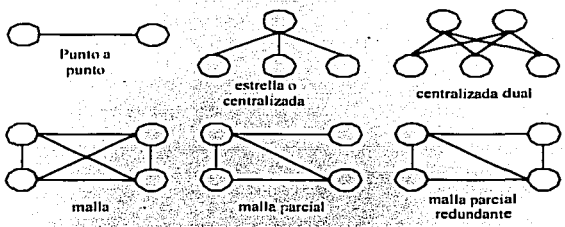


Figura 14. Topologías empleadas para el diseño de arquitectura WAN

Muchos a muchos — malla

En esta topología, cada sitio es capaz de comunicarse con cualquier otro sitio. Un ejemplo puede ser una compañía de compras por correo con una docena de depósitos regionales. Las ordenes pueden ser recibidas y manejadas en cualquier deposito. Si un deposito no tiene el artículo en existencia, la compañía necesita ser capaz de contactar cualquier otro deposito para tratar de satisfacer la orden. Niveles similares de tráfico son esperados entre cualquier par de depósitos, así que no hay un lugar central obvio por el cual transite el tráfico.

Malla parcial

Es una situación intermedia entre una red en estrella y una malla completa. Imaginemos una compañía que tiene que surtir pedidos alrededor del mundo. Hay siete oficinas en diferentes países. La casa matriz de la compañía está en Londres y todas las sucursales comercian frecuentemente con el almacén principal. En consecuencia todas las sucursales tienen conexión hacia Londres. Los vendedores en Alemania regularmente tratan con Paris, así que estos sitios están directamente conectados. Tokio, Singapure y Hong Kong tienen un comercio regional significativo, así que están interconectados. Las transacciones entre todas las oficinas que no están directamente interconectadas son completadas a través de la oficina en Londres. Si un patrón claro de comercio va a ser desarrollado entre un par de oficinas, por decir Alemania y Tokio, la compañía puede considerar su interconexión.

Malla parcial redundante

Esto es una malla parcial, pero con la regla de que cada sitio debe ser conectado al menos con otros dos. Esto permite a un sitio continuar trabajando si uno de los enlaces se pierde. En nuestra red imaginaria, Nueva York puede no ser capaz de trabajar si su enlace con Londres falla. La red puede ser una malla completa instalando en Nueva York una segunda conexión, por ejemplo a Tokio.

Redes jerárquicas

La figura 15 muestra una red jerárquica. Esto es requerido típicamente en redes muy grandes. La red es dividida en regiones. Los sitios en una región son conectados en un sitio central a través de una red regional.

Los sitios centrales son interconectados a través de una red de backbone. Algunos diseños de redes pueden emplear más de dos capas. Las redes públicas son comúnmente diseñadas usando tres o cuatro capas jerárquicas.

Las tecnologías usadas en las redes regionales y la red de backbone pueden ser diferentes, considerando que los sitios centrales deben manejar la transición necesaria.

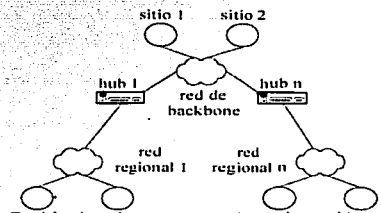


Figura 15. Red jerárquica conectando cada región a un sitio central

Es evidente que cuando se trabaja en este tipo de diseños, el diseñador necesitará tomar en cuenta los siguientes puntos:

- Cuáles sitios necesitan una red local y cuantos son?
- Cuántos sistemas finales van a ser conectados?
- Cómo están distribuidos los sistemas finales en el edificio?
- Cuál va a ser la tecnología LAN principal?
- Cuánto equipo se va a necesitar y como se va a conectar?
- Qué tipo de medio de transmisión se va a utilizar?
- Cuáles son los requerimientos de seguridad? (ej. regulaciones de incendios)
- Los equipos deben ser administrables?
- Qué marca debe ser usada?

Además el diseñador debe mantener en mente las reglas técnicas del diseño asociadas a las tecnologías LAN. Estas son:

- Distancia del cable.
- Número máximo de saltos.
- Número máximo de sistemas finales por red.

3.3. Nombres y direcciones

Muchas redes de datos tradicionales operan en la capa física del modelo OSI, y proveen simples enlaces de bits entre los sistemas finales.

Con el surgimiento de las redes orientadas al switcheo de paquetes se cambió la perspectiva. En estas redes, la información es enviada en bloques conocidos como paquetes. Las decisiones de switcheo en la red son hechas basándose en cada paquete. Para funcionar correctamente, un esquema coherente de direccionamiento debe ser instalado, para que la red pueda hacer las decisiones de ruteo apropiadas.

Una de las primeras tareas del diseñador de red en la etapa de diseño lógico es diseñar el esquema de direccionamiento para la red. Los requerimientos exactos para el esquema dependerán de los protocolos que operarán en la red de alto desempeño, y en caso de soportar múltiples protocolos, el esquema de direccionamiento para cada uno se tendrá que diseñar. Se deberá tener lo siguiente en mente:

- Identificar de forma única a cada sistema final.
- Reflejar la topología de la red. Generalmente esto consistirá en un conjunto de subredes interconectadas por nodos de switcheo o routers.

Una vez que el esquema de direccionamiento ha sido diseñado y documentado a un nivel abstracto, existe la necesidad para un administrador de red de enumerar, registrar y mantener las direcciones actualmente usadas. Las fallas en este proceso pueden tener serias consecuencias en la correcta operación de la red, especialmente ahora que se requiere de agilidad para soportar las redes modernas. Algunos ejemplos de protocolos en donde las direcciones deben ser definidas se presentan a continuación, junto con algunas notas para diseñar el esquema de direccionamiento para cada uno:

- *Direcciones MAC.* Es la dirección en la capa física de cada una de las interfaces en los sistemas finales y equipos de comunicaciones. Usualmente, estas direcciones están grabadas en la tarjeta de red —existen estándares para que cada fabricante tenga su propio segmento de direcciones MAC. Sin embargo esto no siempre se cumple, y algunos sistemas de red requieren que las direcciones MAC sean configuradas manualmente (ej. sistemas SNA de IBM).

- *Token Ring.* Las redes Token Ring tienden a hacer un uso extensivo de la tecnología SRB (Source Route Bridging), que permite que los paquetes sean correctamente dirigidos a través de múltiples segmentos LAN interconectados por bridges. En estas redes, es esencial que el administrador de red asigne un número único de anillo para cada Token Ring. Los números también son asignados a los bridges, pero el único momento en que un bridge necesita un número diferente de 1 es si existen más de un bridge interconectando directamente a los anillos.

- *IP.* Parece inevitable que por lo menos algunas entidades en la red de alto desempeño necesiten dirección IP, aun si la red utiliza bridges y ninguna aplicación final use el protocolo TCP/IP. La razón de esto es la proliferación del protocolo de administración SNMP para los dispositivos de red, ya que éste utiliza IP para comunicarse. Las direcciones IP tienen una longitud de 32 bits (convencionalmente, las direcciones son escritas con los valores decimales de los 4 bytes, separados por puntos.

Clase	Longitud Netid		Longitud Hostid	No. de redes	No. de usuarios
	ID				
A	0	7	24	126	16 777 215
B	10	14	16	16 382	64 516
C	110	21	8	2 097 150	254
D (Formato multifunción)	1110	28	-	-	-
E (Formato futuro)	11110	-	-	-	-

Tabla 4. Clases utilizadas en el esquema de direccionamiento IP

- *Clase A.* Son las que en su primer byte tienen un valor comprendido entre 1 y 126. Estas direcciones utilizan únicamente el primer byte para identificar a la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a la misma red. Esto significa que podrán existir más de dieciseis millones de computadoras en cada una de las redes de la clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que solo puede haber 126 redes de este tamaño.

- *Clase B.* Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1.x.x y 191.254.x.x (no es posible utilizar los valores 0 y 255 por tener un valor especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64,516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el

número de computadoras que se necesitase conectar fuese mayor, sería posible obtener más de una dirección de clase B, evitando el uso de una clase A.

- *Clase C.* En este caso, el valor del primer byte tendrá que estar comprendido entre 192 y 223. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1.x hasta 223.254.254.x. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadoras en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas.

En la tabla 4, en el número de redes, se puede notar que ciertas clases no se usan. Algunas de ellas se encuentran reservadas para un posible uso futuro, como en el caso de las direcciones cuyo primer byte sea superior a 223 (clase D y E, que aún no están definidas).

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red en la que se encuentran conectadas, en la identificación de *host* para máquinas que aún no conocen su número de *host* dentro de la red, o en ambos casos.

El número 225 tiene también un significado especial, puesto que se reserva para el *broadcast* es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso del *broadcast* es cuando se quiere convertir el nombre por dominio de una computadora a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Cuando se diseña un esquema de direccionamiento IP, el administrador debe decidir si la red usará direcciones homologadas o un esquema de direccionamiento privado. Las direcciones homologadas son normalmente adoptadas cuando el usuario tiene la necesidad de ser conectado a Internet. El administrador tendrá que solicitar a las autoridades de Internet (InterNIC o RIPE) un dominio de direcciones registrado (la clase solicitada dependerá del tamaño de la red, en términos del número de usuarios). Note que debido a la rápida expansión del Internet, las direcciones IP son escasas. Las direcciones clase C están normalmente disponibles pero las clase B son usualmente difíciles de obtener y las clase A ya no están disponibles.

Las limitantes del espacio de direcciones IP registradas han sido reconocidas, y el IETF (el cuerpo encargado del desarrollo técnico de Internet) ha desarrollado una nueva generación del protocolo IP, Ipv6 (la versión actual es Ipv4). Este nuevo esquema tiene, entre otras características, un campo más largo para el direccionamiento. Sin embargo IPv6 no se ha implementado por completo.

Por otro lado, cuando no hay necesidad de conectarse a Internet, el usuario puede crear un esquema privado de direccionamiento. Es recomendado que el administrador tome como referencia el RFC 1597 y adopte las direcciones de la clase A, 10.x.y.z. (también hay un rango reservado de direcciones en la clase B y C para su uso en redes privadas no registradas. El Internet está configurado para descartar cualquier paquete portando una dirección de este rango).

El caso más común será una compañía que necesite conectarse a Internet (para proveer a sus empleados el acceso al WWW o correo electrónico). Debido a los riesgos de seguridad asociados a la conexión a Internet, esto siempre debe hacerse de forma controlada (ej. firewall).

En esta etapa, el esquema de direccionamiento define una sola red con muchos usuarios. En realidad, una red de alto desempeño necesitará dividir este espacio en muchas subredes, cada una con sus propias direcciones de subred. Las subredes son interconectadas por routers, los cuales no reenviarán el tráfico destinado a la subred local, y sabrán el mejor camino para reenviar el tráfico a subredes remotas. El administrador de red tendrá que definir el rango de subredes a utilizar. Esto se muestra en la tabla 5.

Red	Subred	usuario
10	x.y.	z

Tabla 5. Esquema propuesto para crear subredes con una red clase A

En la figura 16 se ha decidido usar el rango especificado en el RFC 1597, 10.x.y.z. El administrador ha determinado que nunca habrá más de 254 usuarios en una subred. Por lo que los 8 bits menos significativos corresponden a la dirección del usuario y los 16 bits siguientes pueden utilizarse para soportar hasta 65534 subredes (considerando que las subredes 0.0 y 255.255 son reservadas como identificador de la red y broadcast). Esto es indicado en los routers y sistemas finales por una máscara de red. Esta tiene 0s binarios representando los bits que están reservados para los usuarios. En la figura 16, la máscara es 255.255.255.0 permitiendo crear 4 subredes.

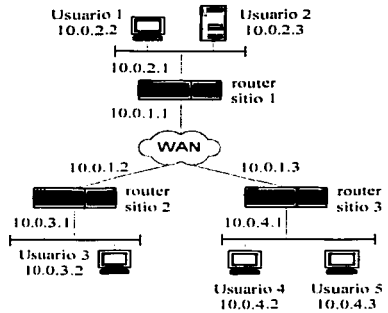


Figura 16. Ejemplo de asignación de direcciones utilizando subredes

El sitio 1 tiene la subred 10.0.2.x con usuarios utilizando las direcciones IP 10.0.2.2 y 10.0.2.3. El router tiene la dirección 10.0.2.1 en su puerto LAN. Una patrón similar de asignación es aplicado a los sitios 2 y 3, junto con la subred WAN.

3.3.1. Consideraciones adicionales

Por supuesto, el diseñador no está obligado a sujetarse a subredes con máscaras de 8 bits. Si decidimos que se necesitan 1022 usuarios para cada subred, podemos usar la máscara 255.255.252.x. De igual forma, si 30 usuarios son suficientes, podemos usar la mascara 255.255.255.224. En la práctica, se recomienda proceder con cautela, porque si una subred se queda sin direcciones disponibles, podría ser necesario renumerar la red completa o asignar más de una subred a cada sitio, lo que redundaría en una mayor carga para los routers. En una red, se puede tener la misma máscara para todas las subredes —esta es la forma más rápida y permite el uso de protocolos más simples. Sin embargo, esto puede ser ineficiente cuando hay sitios de diferentes tamaños. El subneteo de longitud variable es una alternativa pero requiere del manejo de un algoritmo de ruteo más complejo.

3.3.2. DNS

El DNS (Domain Name System) es el método por el cual las direcciones de Internet en forma mnemónica como *telecom.dgsca.unam.mx* son convertidas a su dirección numérica equivalente como 132.248.20.1. Para el usuario y los procesos de aplicación, esta traducción es un servicio proporcionado localmente o por vía remota a través de Internet [bib04]. El servidor DNS puede comunicarse con otros servidores Internet de DNS si no puede traducir la dirección por sí mismo.

El DNS es una base de datos distribuida. Esto permite un control local de los segmentos de toda la base de datos, sin embargo, los datos en cada segmento están disponibles a través de la red por medio del esquema cliente-servidor. Los nombres DNS son construidos jerárquicamente. El nivel más alto de la jerarquía es el último componente o etiqueta de la dirección DNS. Las etiquetas pueden tener hasta 63 caracteres de longitud y no son sensibles a la escritura. Las etiquetas deben comenzar con un letra y solamente pueden consistir de letras, números y guiones (no se recomienda construir nombres que comiencen con números. Esto puede causar problemas con software que simplemente inspecciona el primer caracter de una dirección para determinar si ha sido escrita una dirección IP o un nombre DNS).

Las direcciones DNS pueden ser relativas o descriptivas. Una dirección descriptiva incluye todas las etiquetas y es globalmente única. Una dirección relativa puede ser convertida dependiendo de la información local del dominio. Por ejemplo *abc.telecom.dgsca.unam.mx* es un nombre descriptivo para el usuario *abc* en el dominio *telecom.dgsca.unam.mx*.

Las etiquetas más significativas para un nombre descriptivo son:

- *arpa*. Esta es una característica especial usada para la traducción en reversa, por ejemplo ir de dirección IP hacia una dirección descriptiva de nombre de dominio. Si todo es correctamente configurado una solicitud para *1.4.220.134.in-addr.arpa* regresará *abc.telecom.dgsca.unam.mx*.

- *Código de 3 letras*. El DNS fue originalmente introducido en los Estados Unidos y el componente final de una dirección fue creado para indicar el tipo de organización alojando a la computadora. Algunas de las etiquetas finales de tres letras (edu, gov, mil) sólo se continúan usando por organizaciones basadas en Estados Unidos, las demás pueden ser usadas en cualquier parte del mundo. En algunos países hay subdominios que indican el tipo de organización como *ac.uk*, *co.uk*, *sch.uk* (Reino Unido), *edu.au* y *com.au* (Australia).

- *Código de 2 letras*. El código final de dos letras indica el país de origen y están definidos en el ISO 3166.

Para cualquier grupo de computadoras involucradas en un esquema de nombres DNS habrá una única lista de nombres DNS y su dirección IP asociada. El grupo de computadoras incluidas en la lista es llamada *zona*. Una zona puede ser un lista de dominio nacional, un cámpus de una universidad o inclusive edificios dentro de la misma universidad. Se dice que el servidor de nombres tiene autoridad sobre la zona aunque también puede ser autoridad de múltiples zonas. Una zona es un subárbol del DNS que se administra por separado. Cada zona es dividida en subzonas, por ejemplo facultades, ENEP's, CCH's, etc. La organización responsable de cada zona está a cargo de proveer los servidores de nombres para dicha zona. Cada zona requiere, por lo menos, dos servidores de nombres que respondan preguntas sobre la zona, uno de ellos localizado fuera de la red local, con lo que se provee redundancia. Cuando una computadora es agregada a una zona, el administrador se encarga de registrar su nombre y número IP notificando al servidor de nombres correspondiente. Un servidor de nombres no necesita saber más que la información de zona de la que es responsable, las direcciones de los servidores de las subzonas que define (en caso de que las haya) y las de los servidores de la zona padre de las que depende.

Dentro de las especificaciones del DNS, se definen dos tipos de servidores de nombres, el primario y el secundario. El servidor de nombres primario es el que contiene los archivos de datos de los host que están corriendo en la zona para la cual él es autoridad. El servidor de nombres secundario obtiene los datos de su zona desde otros servidores de nombres, los cuales son autoridad para esa zona, o lo que es lo mismo, de los servidores primarios.

3.3.3. NAT

Uno de los problemas principales al trabajar con Internet es la disminución de direcciones IP. La solución a corto plazo es reutilizar direcciones situando NAT (Network Address Translator) en los bordes de pequeños dominios. Cada caja NAT tiene una tabla consistiendo de pares con direcciones IP locales y direcciones globalmente únicas (homologadas). Las direcciones IP dentro del dominio no son globalmente únicas, son reutilizadas en otros dominios, resolviendo el problema de disminución de direcciones. Las direcciones IP

globalmente únicas son asignadas de acuerdo a los actuales esquemas de asignación [bib10]. Esta solución tiene cabida en lugares en donde hay un porcentaje muy pequeño de usuarios dentro de un pequeño dominio que están comunicándose fuera en un momento dado (un pequeño dominio puede ser una red local que sólo maneje tráfico originado o destinado a los usuarios en el dominio), y solamente un reducido grupo de direcciones IP necesitan ser traducidas a direcciones IP globalmente únicas cuando requieren comunicación hacia Internet.

Esta solución tiene la desventaja de no ser completamente compatible con todas las características que ofrecen las direcciones IP.

La gran ventaja de esta tecnología es que puede ser instalada de forma incremental y muy rápido.

NAT es una función de ruteo que puede ser configurada de la siguiente manera:

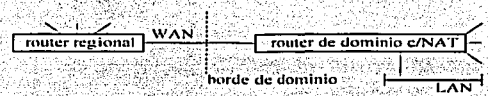


Figura 17. Sitio genérico aplicando NAT a redes locales con conexión WAN

La dirección dentro del pequeño dominio puede ser rehusada por otro dominio (si existe más de un punto de salida es de gran importancia que cada NAT tenga la misma tabla de traducción). Por ejemplo, en la figura 18, ambos dominios A y B usan internamente la dirección clase A 10.0.0.0. El NAT del dominio A tiene asignada la dirección clase C 198.76.29.0 y el NAT B tiene asignada la dirección clase C 198.76.28.0. Las direcciones clase C son homologadas y ningún otro NAT puede usarlas.

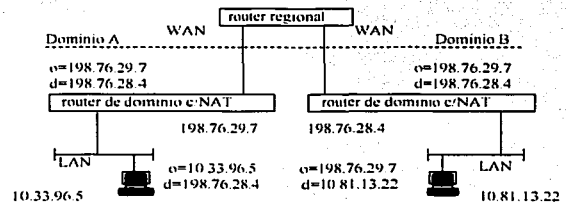


Figura 18. Traducción de direcciones entre sitios con configuración NAT

Cuando el cliente 10.33.96.5 en el dominio A desea enviar un paquete al cliente 10.81.13.22 en el dominio B, éste utiliza la dirección homologada 198.76.28.4 como destino, y envía el paquete a su router primario. El router tiene una ruta estática para la red 198.76.28.0 así que el paquete es reenviado al enlace WAN. Sin embargo, NAT traduce la dirección origen 10.33.96.5 en el encabezado IP con la dirección homologada 198.76.29.7 antes de que el paquete sea reenviado. Los paquetes IP de regreso siguen el mismo mecanismo para la traducción de direcciones.

Note que esto no requiere cambios en los clientes o routers. Por ejemplo, en lo que concierne al cliente en el dominio A, 198.76.28.4 es la dirección usada por el cliente en el dominio B. La traducción de direcciones es completamente transparente.

Por supuesto que esto es un simple ejemplo, por tanto, hay numerosos detalles que deben ser explorados:

- Para que NAT opere correctamente, es necesario dividir el rango de direcciones IP en dos partes, las direcciones locales (direcciones internas reutilizables) y las direcciones homologadas (direcciones

globalmente únicas). Cualquier dirección dada debe ser local u homologada. No deben traslaparse; el problema que podría presentarse es el siguiente. Digamos que un cliente en el dominio A desea enviar un paquete a un cliente en el dominio B, pero la direcciones locales en el dominio B son iguales a las direcciones locales en el dominio A. En este caso, los routers en el dominio A podrían no ser capaces de redireccionar los paquetes.

- Una sola clase A puede ser asignada para redes locales sin conexión a Internet. NAT provee una forma fácil de cambiar una red experimental en una red real traduciendo las direcciones experimentales a direcciones homologadas. Los dominios existentes con direcciones homologadas asignadas internamente, pero comenzando a carecer de ellas, pueden cambiar las direcciones subred por subred. Las direcciones liberadas pueden ser usadas por NAT para comunicaciones externas.

- El router con NAT nunca debe advertir de las redes locales conectadas al backbone. Solamente las redes con direcciones homologadas pueden ser conocidas fuera del dominio. Sin embargo, la información global que NAT recibe del router de frontera puede ser propagada en el dominio de forma usual.

- En muchos casos, una red privada puede estar distribuida en diferentes localidades y usar un backbone público para la comunicacionès entre ellas. Este tipo de dominios deben comportarse como si no estuvieran divididos. Es decir, los routers en todas las particiones deben rutear el rango de direcciones locales de todas las particiones. Por supuesto, los backbones públicos no mantienen ruteo hacia ninguna red local, por lo tanto, los routers de frontera deben transmitir la información a través del backbone usando encapsulación. Para lograr esto, cada NAT debe ser configurado con una dirección homologada. Cuando un NAT x en una partición X desee enviar un paquete a la partición Y, encapsulará el paquete en una cabecera IP con la dirección destino referenciada al NAT y que ha sido reservado para la encapsulación. Cuando el NAT y recibe un paquete con dicha dirección destino, éste desencapsula la cabecera IP y reenvía el paquete internamente.

- Además de modificar las direcciones IP, NAT debe modificar el checksum de IP y TCP (verificación de errores). Debe recordarse que el checksum TCP incluye una pseudo cabecera que contiene la dirección origen y destino. NAT también debe modificar los demás lugares en donde aparezcan direcciones IP.

- Cualquier aplicación que transporte direcciones IP no va a trabajar con NAT a menos que NAT conozca dichas instancias y haga la traducción apropiada. Generalmente, no es posible que NAT conozca todas las aplicaciones.

- Desafortunadamente, NAT reduce el número de opciones para proveer seguridad. Con NAT, nada que transporte direcciones IP o información derivada de una dirección IP (como el checksum TCP) puede ser encriptado. Por otro lado, NAT puede ser visto como un mecanismo de seguridad por el hecho de que las máquinas conectadas al backbone no pueden monitorear cuáles clientes están enviando y recibiendo tráfico. Sin embargo, el otro lado de la moneda es que si un cliente está abusando del Internet en alguna forma (ej. atacar otras máquinas o enviar correo basura) es más difícil localizar la fuente del problema dado que la dirección IP del cliente está oculta.

3.3.4. DHCP

Un problema creciente para los diseñadores es el aumento de los usuarios móviles, remotos y la necesidad por usar eficientemente el rango de direcciones asignado. En todos los casos, el usuario espera ser capaz de conectarse a cualquier servicio de red, en cualquier escritorio y poder acceder a su correo electrónico o navegar en Internet. La respuesta a este problema es utilizar un protocolo llamado DHCP, que permite la asignación dinámica de direcciones IP.

DHCP (Dynamic Host Configuration Protocol, RFC 1541) provee parámetros de configuración a los clientes de Internet. DHCP consiste de dos componentes: un protocolo para enviar parámetros de configuración de un servidor DHCP hacia un cliente y un mecanismo para asignar direcciones de red a los clientes.

DHCP está construido en un modelo cliente-servidor, en donde las máquinas designadas como servidor DHCP contienen direcciones de red y entregan parámetros para configurar dinámicamente a los usuarios. El termino "servidor" está referido a una máquina proporcionando parámetros de inicialización a través de DHCP, y el término "cliente" se refiere a una máquina solicitando dichos parámetros.

Una máquina no debe actuar como servidor DHCP a menos que sea configurado explícitamente por el administrador. La diversidad de hardware e implementaciones de protocolo en el Internet podría comprometer la operación confiable si máquinas aleatorias pudieran responder a las peticiones DHCP. Por ejemplo, IP requiere de la configuración de varios parámetros dentro de la implementación del protocolo. Debido a que IP puede usarse en diferentes equipos de red, los valores para dichos parámetros no pueden ser asumidos o adivinados. También, los distintos esquemas de asignación de direcciones dependen de un mecanismo de revisión/defensa para descubrir las direcciones en uso. Los usuarios IP no siempre pueden ser capaces de defender su propia dirección de red, así que dichos esquemas no pueden garantizar el evitar asignar direcciones de red duplicadas.

DHCP soporta tres mecanismos para asignar direcciones IP. En "asignación automática", DHCP proporciona una dirección IP permanente a un usuario. En "asignación dinámica", DHCP proporciona una dirección IP aleatoria por un periodo limitado de tiempo (o hasta que el usuario renuncie explícitamente a la dirección). En "asignación manual", la dirección IP del usuario es proporcionada por el administrador de red, y DHCP es usado simplemente para entregar la dirección asignada. Una red en particular puede usar uno o varios de estos mecanismos, dependiendo de las políticas definidas por el administrador.

La asignación dinámica es el único mecanismo que permite reutilizar cualquier dirección que ya no sea necesitada por el usuario al cual previamente se asignó. Por lo que, es particularmente útil para asignar una dirección a un usuario que va a estar conectado a la red solo temporalmente o para compartir un grupo limitado de direcciones IP entre un grupo de usuarios que no necesiten direcciones IP permanentes. También puede ser una buen opción para asignar una dirección IP a un usuario nuevo y permanente en lugares en donde las direcciones sean escasas y sea imperativo recuperar las direcciones de usuarios retirados.

Hay varios protocolos de Internet y mecanismos relacionados que solucionan parte del trabajo de configurar usuarios. Ejemplos son: RARP (Reverse Address Resolution Protocol) que explícitamente soluciona el problema de descubrir direcciones de red e incluye un mecanismo automático de asignación IP, TFTP (Trivial File Transfer Protocol) que proporciona el transporte de la imagen *boot* desde un servidor de inicialización e ICMP (Internet Control Message Protocol) que informa a los usuarios de caminos adicionales, máscaras de red utilizadas y routers.

La siguiente lista proporciona características generales de DHCP:

- DHCP debe ser un mecanismo en lugar de una política. DHCP debe permitir a los administradores locales tener control sobre los parámetros de configuración en donde se necesite, por ejemplo, los administradores deben ser capaces de modificar las políticas de asignación y acceso a los recursos.

- Las máquinas no requieren configuración manual. Cada máquina debe ser capaz de descubrir los parámetros locales de configuración sin la intervención del usuario e incorporar dichos parámetros en su configuración.

- Las redes no requieren configuración manual para máquinas individuales. En circunstancias normales, el administrador de red no debe trabajar en parámetros de configuración por cada máquina.

- DHCP no debe requerir un servidor por cada subred. Para permitir escalabilidad y economía, DHCP debe trabajar a través de routers.

- Un servidor DHCP debe estar preparado para recibir múltiples solicitudes por parámetros de configuración. Algunas instalaciones pueden incluir varios servidores intercomunicados para incrementar la confiabilidad y el rendimiento.

- DHCP debe convivir con máquinas configuradas estáticamente y no participantes y con implementaciones previas de otros protocolos.

3.4. Ruteo

Una vez determinado el esquema de direccionamiento, tenemos que decidir como los routers van a adquirir la información necesaria para enrutar los paquetes con información del usuario a través de la red. Esto es logrado seleccionando y configurando el protocolo de ruteo apropiado. Estos protocolos son responsables del intercambio de información entre routers, y ayudarse mutuamente a construir la tabla de ruteo.

Existen diferentes protocolos, cada uno con ventajas y desventajas. Seleccionar el óptimo es una de las decisiones claves en el proceso de diseño lógico. A continuación se describen diferentes opciones sobre protocolos de ruteo:

3.4.1. Ruteo estático

En esta característica en apariencia trivial, el ruteo es logrado a través de configuraciones codificadas explícitamente en las tablas de cada router.

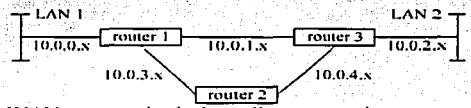


Figura 19. Red WAN con topología de malla para emplearse con ruteo estático

Tomando el ejemplo de la figura 19 y considerando que el tráfico fluye entre LAN1 y LAN2, el router 1 va a necesitar una configuración de ruteo estableciendo que la subred 10.0.2.x será alcanzada enviando los paquetes a través de su puerto WAN en la subred 10.0.1.x. De igual forma, para regresar el tráfico, el router 3 va a necesitar una configuración indicando que la subred 10.0.0.x puede ser alcanzada a través de su puerto WAN en la subred 10.0.1.x. El ruteo estático no puede hacer un uso efectivo de los enlaces redundantes, así que cualquier conexión a través del router 2 no va a aparecer en la configuración.

El ruteo estático tiene la ventaja de ser relativamente simple de configurar en redes pequeñas, y no requiere de mucha capacidad de procesamiento, también puede ser valioso cuando la seguridad es imprescindible ya que se conoce exactamente como fluye el tráfico en la red. No hay oportunidad para algoritmos de ruteo dinámicos para descubrir enlaces inseguros no previstos o conexiones de sistemas externas que pretendan averiguar la configuración general de la red.

Así como el ruteo estático tiene algunas ventajas, las desventajas son de cierta importancia debido a que pueden relegar esta forma de ruteo en situaciones especiales. Las desventajas son:

- *Poca escalabilidad.* Conforme se agreguen nuevas redes, todos los routers que necesiten comunicarse, o estén envueltos en el tráfico requerirán ser configurados manualmente. Con redes mayores a una docena de routers, la tarea se vuelve impráctica.
- *Sin redundancia.* Una ventaja clave de los protocolos de ruteo dinámico es que las redes se pueden autoreparar descubriendo enlaces alternativos hacia las redes destino. Las redes con ruteo estático no pueden tomar este tipo de ventaja.

3.4.2. Ruteo dinámico — protocolos Distance Vector

RIP (Routing Information Protocol) de TCP/IP es un ejemplo clásico de este tipo de protocolos. Los routers son configurados con la lista de subredes directamente conectadas al router. Periódicamente el router hará un llamado a todos los routers conectados a las subredes, informando de las subredes que pueden ser

alcanzadas. Cuando un router recibe una actualización de ruteo de un vecino, la actualización va a contener información acerca de las subredes no directamente conectadas al router destino. El router va a añadir esta nueva información adquirida en la tabla de ruteo. Cuando este router envíe su propia actualización, llevará la información sobre las redes que acaba de aprender. Este proceso es repetido hasta que, eventualmente, todos los nodos hayan aprendido rutas hacia todas las subredes.

De acuerdo a lo anterior, dos desventajas de los protocolos de ruteo dinámico son claras. Primero, estos utilizan cierto ancho de banda al momento de enviar la información de actualización y segundo, requieren tiempo de proceso en los routers para enviar y recibir estas actualizaciones.

Distance Vector

Para explicar el protocolo Distance Vector, consideremos el siguiente ejemplo. Tomemos la red mostrada en la figura 19. Así como las direcciones de las subredes que pueden ser alcanzadas, la actualización de ruteo contiene información acerca de la "distancia" hacia la subred. Con RIP, esto es simplemente expresado como el número de saltos (ej. el número de routers que debe pasarse para llegar a la subred destino). Así que la actualización procede como sigue para el router 1 (los demás operan de la misma forma):

actualización	Subredes conocidas	Número de saltos
Condición inicial	Subredes localmente conectadas	
	10.0.0.x	0
	10.0.1.x	0
	10.0.3.x	0
Después de actualización	Subredes existentes y agregadas	
1 de routers 2 y 3	10.0.0.x	0
	10.0.1.x	0
	10.0.3.x	0
	10.0.2.x	1 (por 10.0.1.x)
	10.0.4.x	1 (por 10.0.3.x)
Después de actualización	Subredes existentes y agregadas	
2 de routers 2 y 3	10.0.0.x	0
	10.0.1.x	0
	10.0.3.x	0
	10.0.2.x	1 (por10.0.1.x)
	10.0.4.x	1 (por 10.0.3.x)
	10.0.2.x	2 (por 10.0.3.x)

Tabla 6. Ejemplo de la actualización de ruteo con la lista de las redes directamente conectadas y alcanzables mediante otros routers

RIP es un protocolo muy simple, capaz de usar solamente el número de saltos para determinar el mejor camino a través de un red. Consideremos el escenario de la figura 20.

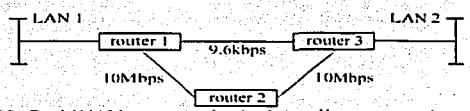


Figura 20. Red WAN con topología de malla para emplearse con RIP

En este ejemplo, los router 1 y 3 están unidos por un enlace serial de 9.6kbps. Los routers también están interconectados por el router 2, en donde el router 1 está enlazado al router 2 a través de un segmento Ethernet dedicado de 10Mbps, de la misma forma que el router 2 al 3, basándose únicamente en la cuenta de saltos, RIP podría escoger enviar el tráfico de LAN 1 a LAN 2 a través del enlace de 9.6Kbps. La decisión tomada no es la mejor. En realidad, se puede configurar manualmente en los routers 1 y 3 que añadan un salto a la ruta de 9.6 Kbps pero este manejo es indeseable y se vuelve increíblemente difícil en redes de gran tamaño.

Existe un cantidad importante de variantes propietarias del protocolo Distance Vector que solucionan esta limitante (ej. Novell RIP y Cisco IGRP). Ambos reemplazan la simple cuenta de saltos asociando un costo a cada enlace de red. Esta métrica es entonces enviada a todos lo routers en el enlace. Los costos son calculados por algoritmos propietarios basados en ciertos factores. Estos incluyen ancho de banda, latencia total y confiabilidad. El algoritmo de ruteo selecciona un camino hacia su destino, basado en el costo total menor y no sólo en la cuenta de saltos.

3.4.3. Ruteo dinámico — protocolos Link State

Los protocolos de ruteo Distance Vector utilizan mucho ancho de banda al enviar continuamente actualizaciones de ruteo. en contraparte, una generación de protocolos de ruteo ha sido creada y denominada Link State. La versión TCP/IP es conocida como OSPF (Open Shortest Path First). Durante su trabajo normal y cuando la red arranca por primera vez, los routers intercambian mensajes de "hello" con sus vecinos para checar que los enlaces funcionan correctamente. Con esta información, un router es capaz de calcular un mapa completo de la red. Solamente si un intercambio de hello falla entonces los routers entran a un proceso de recálculo, en donde todos los routers van a recalcular la topología.

La desventaja de los protocolos Link State es que el proceso de recálculo es complicado y se necesitan routers con más poder de procesamiento y mucha memoria, periodo durante el cual la red no transmite tráfico. En general, la recuperación después de una falla en la red es más rápida que con Distance Vector.

3.4.3.1. Escalabilidad

Con los protocolos Link State, el tiempo tomado para recalcular el mapa de la red se incrementa de manera proporcional al número de routers en la red. Esto en principio, puede hacer que escalar las redes pueda ser un problema. La realidad es que los protocolos Link State fueron diseñados con la escalabilidad en mente, y esto es hecho dividiendo las redes en áreas. Un área es un grupo de routers compartiendo el mismo proceso de recálculo. Las áreas son unidas con routers de frontera (los cuales generalmente son conectados a un máximo de tres áreas). Los routers de frontera también realizan el proceso de recálculo.

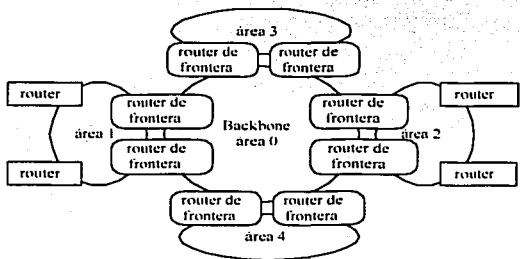


Figura 21. Areas utilizadas por el protocolo link state para permitir escalabilidad

En la figura 21, hay un área central de backbone 0 con un conjunto de routers interconectados. El área 1 es también un conjunto de routers enlazados en la nube. Las áreas 0 y 1 comparten dos routers de frontera (un router entre fronteras es suficiente, pero las redes grandes usualmente conectan dos para evitar un sólo punto de falla). El área 2 está igualmente conectada al núcleo. En un red típica, los hubs o switches son generalmente asociados con routers al área de backbone. Cualquier tráfico entre áreas debe pasar por el área de backbone.

Utilizando esta técnica de múltiples áreas, las redes pueden, en principio, ser escaladas a cientos de sitios. En la red mostrada en la figura 21, podemos incrementar significativamente la eficiencia del proceso de ruteo simplificando el intercambio de información sobre direcciones IP (con una selección cuidadosa del esquema

de direccionamiento que refleje la estructura del área de ruteo). Si mantenemos el esquema de direccionamiento 10.x.y.z asumiendo que x = número de área, y = subred y z = sistema final, los routers de frontera pueden mejorar el intercambio de información ya que sólo necesitaran decirle a los demás routers que pueden ver la red 10.x en lugar de proporcionar una lista con todas las subredes en 10.x.y.

3.4.3.2. Sistemas autónomos

Una red OSPF formada por un backbone y sus áreas representa un sistema autónomo. El mismo protocolo de ruteo OSPF es descrito como un protocolo de ruteo de compuerta interior. Los sistemas autónomos pueden ser interconectados usando un protocolo de compuerta exterior el cual podría funcionar conectando a cada red OSPF [bib04]. Estos routers de compuerta de los sistemas autónomos son interconectados a través de una red de backbone. Para obtener redundancia en la red, uno podría tener por lo menos dos compuertas por sistema autónomo. El principal protocolo de compuerta exterior usado hoy día es BGP4. (BGP4 puede aplicarse a la compuerta exterior, eBGP, e interior, iBGP).

BGP4 está diseñado para comunicar solamente información simplificada de las redes conectadas al router de compuerta del sistema autónomo. Por esto, es muy efectivo conteniendo problemas de ruteo dentro de los sistemas (autónomos). Digamos que una subred dentro de un área OSPF aparece y desaparece debido a una falla en la conexión WAN. La información de cada transición circulará alrededor del sistema autónomo, originando un gran incremento en el tráfico que requerirá de mucho procesamiento en los routers. Debido a que BGP4 solamente pasa información acerca de la disponibilidad de toda la red, el incremento ocasionado por la inestabilidad en el enlace no se propagará hacia las otras redes.

Idealmente, uno diseña sistemas autónomos de tal forma que la mayoría del tráfico va a ser soportado dentro del sistema autónomo, y solamente una pequeña cantidad cruza entre los sistemas. Esto mantiene el tráfico que los routers tienen que transmitir al mínimo y también ayuda a evitar que los routers de compuerta se conviertan en un cuello de botella.

La figura 22 muestra una típica red con múltiples sistemas autónomos. Hay cuatro universidades, cada una con su propia red. Los cámpus utilizan ruteo OSPF. Las universidades han decidido interconectar sus redes para poder compartir información, correo electrónico, etc. Esto es logrado con una red de backbone inter-universidades, la cual emplea BGP4.

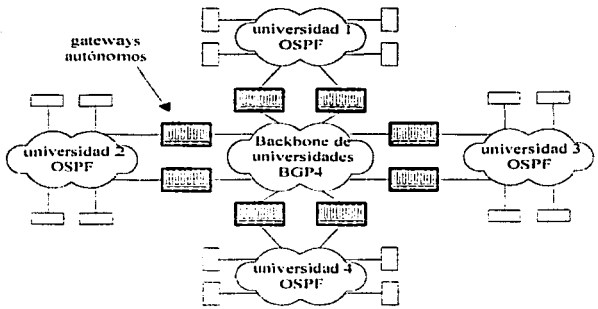


Figura 22. Típica red con múltiples sistemas autónomos

3.5. Seguridad

Todas las redes son objetivos potenciales de ataques con malicia, por simple curiosidad, hackers y crackers. Esto puede ser tan simple como alguien robando información personal y vendiéndola, o tan directo como un ataque a los registros de un banco.

La seguridad es un tópico serio que el diseñador no puede dejar de lado. Los incidentes de seguridad mayores son registrados por CERT y reciben aproximadamente 2500 incidentes al año.

La seguridad en la red tiene que ver con resguardar las operaciones y preservar la integridad ante un daño accidental o un ataque deliberado. Hay muchos aspectos que conforman la seguridad, desde la privacia (la habilidad para guardar secretos), la integridad, hasta las tres A, autenticación (saber quién es cada uno), autoridad (permitir ejecutar sólo ciertas funciones) y auditoria (saber qué pasó, quién lo hizo y cuándo). Dada esta panorámica, es sumamente importante la protección de las redes de alto desempeño de ataques. Definitivamente, el diseñador necesitará buscar la ayuda de los expertos en la materia, pero hay un nivel base de consideraciones que debe tener y una serie de precauciones que puede tomar por sí mismo.

3.5.1. Esquema general

Antes de que podamos comenzar a diseñar la seguridad en nuestra red, debemos entender el nivel de intercambio al cual va a estar expuesta, y los tipos de ataque que pueden ser usados. Una vez comprendido, podemos pensar en que seguridad adicional puede ser construida en la red de alto desempeño para protegerla contra los ataques.

Muchas redes van a requerir diseños de red basados en estándares formales cuyo trabajo tendrá que ser elaborado por un consultor especialista en estas metodologías.

Por supuesto, el diseñador de red debe mantener en mente la seguridad durante el proceso de diseño [bib04], para que éste pase las auditorias posteriores sin (o con pocas) modificaciones. El diseñador deberá realizarse las siguientes preguntas:

¿Quién puede atacar la red y porqué?.

- *Internos*. Por un usuario con beneficio personal o malicia.
- *Externos*. Como un hacker tradicional el cual disfruta del reto de atacar sistemas.
- *Indirectos*. Una compañía que recibe un correo electrónico con virus y éste se autoenvía.

¿Qué componentes pueden ser atacados?.

- *Elementos de red*. Routers, hubs, switches, sistemas finales, etc.
- *Servidores de accesos remoto (dial up)*.
- *Sistemas operativos*. Unix, Winx.
- *Servidores de correo y las aplicaciones que residen en él*.

¿Qué tipo de ataque puedo esperar?.

- *Ataque directo*. Ingresar a las aplicaciones y utilizarlas como un usuario legítimo para propósitos distintos. Ej. robar u otorgar contraseñas.

- *Negación de servicio*. Evitar que la red y las aplicaciones operen correctamente. Hay varias opciones, como el ancho de banda (usando dispositivos como el "ping de la muerte"), sockets de TCP/IP (usando TCP SYN), poder de CPU (usando land.c y Teardrop), memoria, espacio en disco, etc.

- *Perdida de privacidad*. Capturar la información y usarla para afectar los intereses del usuario. Los sniffers están enteramente disponibles y pueden usarse para estos propósitos.

- *Modificación de información.* La información puede ser modificada (ej. cambiar las cantidades en una transacción monetaria).

- *Mascarada.* Pretender ser el destino legitimo. Puede ser un sitio web con un URL similar, diseñado para difamar la información original. Puede ser un simulador, engañando a los usuarios para que revelen sus contraseñas.

- *Búsqueda de información.* Usualmente el preludio a alguno de los ataques anteriores. Las herramientas básicas de TCP/IP como ping o traceroute pueden ser usadas. Herramientas de escaneo sofisticadas pueden ser usadas para buscar sistemáticamente por vulnerabilidades en la seguridad. Muchas de estas herramientas pueden descargarse gratuitamente del Internet.

¿Cuáles son los métodos de defensa?

- *Confidencialidad.* Asegurar que la información está protegida contra la perdida de privacía, a través del uso de encripción.

- *Integridad.* Proteger contra modificaciones a la información añadiendo firmas electrónicas seguras a los mensajes.

- *Autenticación.* Proteger contra ataques directos a través de pruebas de seguridad de tal forma que el usuario conectado sepa que el sistema es genuino. También se puede proteger de manera similar contra una mascarada.

- *Disponibilidad.* Usar diseños redundantes para servidores que fortalezcan la protección contra ataques de negación de servicio. Técnicas simples como los respaldos son importantes para mejorar la velocidad de recuperación después de un ataque exitoso.

- *Auditoria.* Mantener registros de las conexiones y sus actividades para detectar ataques y prevenir que vuelvan a ocurrir.

3.5.2. Soluciones para la seguridad en la red

La primer pregunta que el diseñador debe hacer es: ¿a qué capa del modelo OSI de 7 capas deben ser implementadas las técnicas de seguridad?. La mejor seguridad va a ser obtenida cuando las técnicas son implementadas en varias capas del modelo. Esto puede involucrar múltiples niveles de acceso (ej. una contraseña para entrar a un servidor y otra para entrar a una aplicación particular) y las posibilidades de un hacker de pasar varias capas de protección sean considerablemente menores que aquellas que brindan una sóla contraseña.

Antes de observar a detalle los pormenores de algunas tecnologías disponibles para implementar soluciones específicas de seguridad, vale la pena repasar donde puede ser insertada la seguridad (las varias capas de una red que pueden ser protegidas de un ataque) [bib04].

3.5.2.1. Seguridad en capa de aplicación

La seguridad más efectiva será diseñada en la capa de aplicación.

- *Confidencialidad.* El software de aplicación puede encriptar la información para su almacenamiento y/o antes de la transmisión entre el cliente y el servidor.

- *Integridad.* El software de aplicación puede agregar firmas electrónicas a los mensajes.

- *Autenticación.* Los usuarios van a ser requeridos para identificarse en los sistemas operativos y aplicaciones. Esto es usual a través del nombre de usuario y contraseña. La seguridad es mejorada cuando las reglas de longitud de la contraseña, diseño y tiempo de vida son implementadas, haciendo a las contraseñas difíciles de adivinar por el atacante. La seguridad se mejora cuando la contraseña es usada en conjunto con pruebas, algo que sabe el usuario y algo que tiene. La prueba puede generar números aleatorios, sincronizados con algún proceso en el sistema final, crear una llave y compartirla para verificar si la información es válida.

- *Disponibilidad.* El software de aplicación debe ser respaldado regularmente. Idealmente la aplicación está disponible desde múltiples servidores en diferentes sitios.

- *Auditoría.* Los sistemas operativos y las aplicaciones deben ser usados para mantener dichos registros.

El diseñador de red frecuentemente no tiene responsabilidad para la selección y el diseño de aplicaciones. Usualmente, la seguridad en la capa de aplicación no es suficiente y por lo tanto debe ser incrementada por la red. Esto puede ser porque las aplicaciones heredadas son usadas sin tener un diseño adecuado de seguridad para usarse en ambientes de red o porque no representan el costo-beneficio suficiente como para invertir en procesamiento más poderoso capaz de soportar la demanda de la seguridad criptográfica.

3.5.2.2. Seguridad en capa de sesión

Generalmente, las aplicaciones seguras van a ser las orientadas a sesión por naturaleza, con el usuario estableciendo una sesión vinculándose con el sistema remoto. Verificaciones como el sondeo periódico del estatus y la secuencia numérica de los mensajes pueden ser usados para asegurar integridad en la sesión (ej. detectar si el usuario original ha sido cortado a la mitad de la sesión y un intermediario está en su posición).

Seguridad adicional puede aplicarse al iniciar la sesión. Esto puede ser en el sentido de un sistema en el cual el usuario envía un número aleatorio el cual debe ser encriptado por el sistema de usuario bajo una llave secreta. La respuesta es verificada para saber si el usuario tiene la llave correcta. Otros sistemas requieren que el usuario posea una ficha la cual genera contraseñas de un sólo uso.

Cada vez más, las redes están usando servidores de seguridad estandarizados los cuales van a reconocer a los usuarios que desean entrar a los sistemas y les van a dar una prueba criptográfica para ser usada al solicitar acceso en la aplicación. Si se va a usar tal servidor de seguridad, el diseñador debe proveer la conectividad de red necesaria, y asegurar que todos los posibles usuarios puedan enviar tráfico a éste.

3.5.2.3. Seguridad en capa de red

Muchos protocolos de la capa de red proveen mecanismos de seguridad útiles. Algunos de los más comunes son:

- *Redes privadas y redes privadas virtuales.* La mayoría de los ataques a la seguridad vienen de las redes de datos públicas como Internet. Cuando la red de alto desempeño no necesita comunicarse con otra red, o no está ofreciendo un servicio público y muy altos niveles de seguridad son buscados, puede justificarse una red privada. Hay un punto débil, sin embargo, en redes ofreciendo acceso telefónico se da la posibilidad al hacker de conectarse a un sistema desprotegido.
- *Grupos cerrados de usuarios.* Estos arreglos son encontrados en redes conmutadas como X.25. Cuando las llamadas son establecidas, los usuarios pueden limitar a un número de usuarios en el grupo. El administrador de red acordará con el proveedor del servicio cuales conexiones de red son miembros del grupo. La llamada dirigida hacia el grupo no puede ser aceptada de un usuario externo que no es miembro. Estos grupos se basan en tablas programadas en la red, las cuales sólo pueden ser cambiadas por el proveedor.
- *Identificación del solicitante.* Cuando una llamada es establecida, la solicitud de llamada va a contener la dirección de red del que llama. La red va a asegurar que esta dirección es la correcta para el circuito físico del cual provino. Los sistemas pueden mantener una lista de direcciones origen aceptables, y descartar llamadas de otras direcciones.

- *Firewalls*. Es una forma de seguridad generalmente asociada con redes de alto desempeño que están conectadas a Internet. También es usada cuando algunas partes necesitan tener sus aplicaciones e información protegidas de los usuarios comunes.

  En su forma más simple, un firewall puede consistir de un router configurado con una lista de acceso, el cual sólo permitirá el tráfico de ubicaciones predefinidas. Las listas de acceso también pueden ser programadas para permitir que el tráfico sea direccionado a usuarios específicos.

  Un firewall debe proveer un número de funciones incluyendo:
  - Encripción.
  - Administración de sesión con verificación de contraseña de usuario.
  - Compuerta de traducción de direcciones (la red destino no usa direcciones de Internet homologadas).
  - Agentes proxy (en aplicaciones como servidores WWW, donde cada petición de acceso es revisada para ver si la página seleccionada está disponible para el usuario en particular).

3.5.2.4. Seguridad en capa de enlace

Un mecanismo comúnmente usado en la capa de enlace en redes basadas en TCP/IP es el protocolo PPP. Este estándar incluye mecanismos de seguridad llamados CHAP y PAP, los cuales pueden ser útiles cuando se usa conectividad con acceso telefónico. Como parte del proceso para establecer un enlace, el solicitante envía una contraseña la cual es verificada por el equipo que recibe la llamada. Este intercambio es realizado de forma transparente para el usuario.

3.5.3. Tecnología para la seguridad

Hay muchos dispositivos que pueden proteger una red y muchos proveedores especialistas en equipamiento de seguridad, sin embargo, hay también un número de personas que están interesadas en romper los esquemas de seguridad.

3.5.3.1. Encripción

El rol principal de la encripción es asegurar la privacía de la información cuando transita a través de las redes públicas. Una de las formas más efectivas para proteger una red puede ser encriptar toda la información fluyendo sobre ésta para que ningún dato intelegible esté disponible al hacker.

Idealmente, la información debe ser encriptada en los sistemas finales. Otra solución de compromiso es encriptar los datos en routers especiales o equipo independiente de encripción en los sitios de trabajo. Los encriptadores orientados a paquetes son también conocidos como encriptadores de carga ya que sólo encriptan los datos del usuario, dejando las cabeceras de los protocolos limpias para que los paquetes puedan ser apropiadamente enviados a través de la red.

El uso exitoso de la tecnología de encripción dependerá del hospedaje seguro de los encriptores y una adecuada administración de las llaves de encripción (incluyendo su cambio regular). Hay dos formas básicas de lidiar con la administración de llaves. La primera es la encripción simétrica donde la seguridad de la encripción depende de un secreto compartido que sólo las dos partes comunicadoras saben. El Algoritmo IDEA (International Data Encryption Algorithm) y el DES (Data Encryption Standard) son ejemplos de sistemas de llave privada. La solución alternativa es la encripción asimétrica donde el usuario tiene un par de llaves, una privada y otra pública. Un mensaje encriptado usando la llave pública solamente puede ser desencriptado usando la llave privada. Así que se pueden recibir mensajes de cualquiera que conozca la llave pública del destino. Los sistemas de llave pública mejor conocidos son Diffie Hellman y RSA (Rivest, Shamir y Adleman).

A pesar de todo lo bueno, hay algunas barreras importantes en el uso de la encripción. La mayor es obtener actualmente el hardware y software necesario para soportar la carga significativa de procesamiento para la encripción. Debido a que los encriptores pueden tener un uso militar, su venta y exportación está rigurosamente controlada. Tal vez el ejemplo mejor conocido de tal restricción es DES, el cual está

clasificado como munición en el Gobierno de Estados Unidos y por lo tanto es objeto de restricciones en su exportación. El diseñador va a tener que investigar ampliamente sobre las limitaciones de licencia antes de seleccionar la tecnología de encripción a utilizar.

El último estándar creado para proveer túneles encriptados seguros a través del Internet es IPSec. Los encriptores son cargados con grupos de direcciones IP origen y destino o subredes, cada grupo constituyendo una Intranet o VPN. A menos por una configuración especial, el encriptador no permitirá que el tráfico pase entre Intranets o VPNs, y usará diferentes grupos de llaves criptográficas para cada red por separado. Los encriptores IPSec tienden a proveer el paquete más conveniente, convergiendo muchas de las áreas de defensa mencionadas antes:

- *Control de acceso*. El encriptor puede mantener un lista de las subredes permisibles.
- *Autenticación*. Confirmar que la información viene de la ubicación que dice venir.
- *Integridad*. La información no debe ser dañada o modificada en tránsito.
- *Sin reenvíos*. Secuencia numérica y marcas de tiempo pueden ser usadas para prevenir retransmisiones impropias en una transacción.

Todos los algoritmos están basados en matemáticas complejas usando problemas en los que se sabe que no tienen solución algorítmica. Estos problemas solamente pueden ser atacados mediante técnicas "*sledge hammer*" que requieren tiempo exponencial en relación a la longitud de la llave a resolver. Un factor primordial en la selección de un sistema de llave pública es la eficiencia.

3.5.3.2. Llaves públicas

Los algoritmos de encripción asimétrica forman la base de la infraestructura de llave pública. Como se mencionó anteriormente, los esquemas de llave pública son ampliamente usados para firmas electrónicas de documentos y para intercambiar llaves de encripción de datos. Un usuario generará un par de llaves pública/privada y dará a conocer la pública. Sin embargo, necesitamos saber que la llave pública pertenece a la persona correcta y no a un impostor. La infraestructura de llave pública logra esto teniendo una tercera parte confiable que verifica la llave pública del usuario, después de que éste le proporcionó su identidad. Esta llave comprobada es llamada certificado, y es entregada por una Autoridad Certificada (Certified Authority, CA).

Un certificado por sí mismo es básicamente un grupo de elementos de datos, conjuntados y verificados electrónicamente por una AC confiable usando su llave privada.

Un certificado básico clase 1 relaciona el nombre de usuario con la dirección de correo electrónico y su llave pública. Es usado por usuarios individuales de Internet para enviar correo seguro o para identificarse a si mismos en servidores WWW.

Un certificado clase 2 es liberado por una organización como un banco, para identificar a sus clientes. Este liga mayores detalles como el número de cuenta.

Los operadores de servidores WWW buscan por un certificado clase 3. En esta instancia, el AC va a ejecutar verificaciones rigurosas para confirmar la identidad del propietario del servidor y que ellos son una organización acreditable. El certificado relaciona el URL de los servidores, el nombre de la organización y su llave pública. Si un servidor tiene dicho certificado, los usuarios de navegadores pueden confirmar que se están comunicando con un servidor genuino y no con un impostor. Más importante, el certificado permite que las llaves de encripción sean intercambiadas y corran sesiones de HTTP seguras (ej. comercio electrónico y transacciones bancarias).

Un aspecto importante del diseño con las llaves públicas es cuando deben ser almacenadas. En una PC, una llave solamente prueba que el mensaje realmente venga de la PC, no la persona. Simples contraseñas de usuario son usadas para proteger la llave privada en la PC, lo que representa una protección débil. Una opción mucho mejor es mantener las llaves privadas en una tarjeta inteligente que se mueva de máquina en máquina con el dueño de la llave. Todas la operaciones de proceso que involucren la llave privada toman lugar en la

tarjeta inteligente, y no hay posibilidad de extraer la llave privada de la tarjeta en ningún momento. Cuando pequeños secretos (llaves) son usados para proteger grandes secretos (información), es una mejor opción de diseño, similar a la idea de mover el procesamiento de los datos seguros.

3.5.3.3. Firewalls

Una de las estrategias más efectivas y ampliamente usadas para preservar la seguridad es usar un sistema firewall. La idea básica es que las máquinas y las redes dentro del firewall son confiables, y los de afuera son generalmente no confiables.

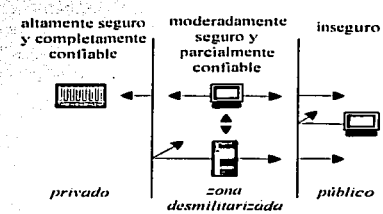


Figura 23. Comunicación entre máquinas dentro y fuera de la red del firewall

Todas las comunicaciones entre máquinas dentro y fuera de la red pasan a través del firewall. Es trabajo del firewall monitorear y filtrar todo el tráfico pasando por él y sólo permitir la comunicación correspondiente a ciertos servicios predefinidos o sistemas externos confiables. Por lo tanto, el tráfico entrante puede ser configurado para permitir el acceso solamente a los privilegiados y el tráfico de salida puede ser limitado si hay ciertos lugares indeseables.

Las máquinas dentro del firewall tienen un grado razonable de confianza y por lo tanto tienen que aplicar menor control entre ellas. Usualmente, secciones de una red interna emplearán por sí mismas firewalls para restringir el dominio de máquinas confiables. Este arreglo es usualmente aplicado dentro de las redes de alto desempeño para dar capas de protección a la información. Con el crecimiento de las extranets, un esquema similar es utilizado para crear zonas desmilitarizadas (Demilitarized Zones, DMZs), donde la información compartida entre organizaciones está protegida del mundo pero continúa disponible para cualquier Intranet o VPN.

Los productos firewall son cada vez más capaces de proveer encripción y esto es usado para crear túneles seguros sobre redes públicas como Internet. Los encriptores están incrementando sus capacidades para decidir que rechazar, pasar tal cual o encriptar, basado en reglas. Estas reglas pueden abarcar las direcciones fuente, direcciones destino, tipo de protocolo e información de la capa de transporte. Por lo tanto, hay una tendencia para que los firewalls y los encriptores convergan.

3.5.3.4. Seguridad para acceso remoto

Los servicios de acceso remoto (aquellos que necesitan de la marcación del usuario en una red) son particularmente objeto de ataques. Hemos mencionado algunas de las características de la protección, como sesión protegida por contraseña o identificación por una tercera parte. Un par más de técnicas útiles asociadas con redes de acceso remoto son:

- *Retorno de llamada.* El usuario va a hacer una conexión telefónica al sistema y pasa a través de una contraseña inicial para tener acceso. En este punto, el sistema va a terminar la llamada. El sistema va a mantener una tabla con el nombre y contraseña del usuario, asociado con los números telefónicos desde los cuales puede llamar. El sistema entonces marca al usuario con el número aprobado para permitir que la sesión continúe. Esta puede ser una buena forma de protección cuando una tercera parte identificante

no es posible (ej. líneas telefónicas analógicas). No conviene su uso cuando los usuarios tienden a ser móviles (y por lo tanto el número telefónico desde el cual llaman no es conocido).

- *Prevención de desconexión.* Un área de mayor riesgo para los accesos telefónicos es cuando un usuario legal completa una llamada. Si la red no está adecuadamente diseñada, puede ser posible para un usuario inapropiado conectarse al mismo puerto inmediatamente después, obteniendo la sesión del usuario legal y continuándola. Esto ocurre especialmente cuando los usuarios no se desconectan apropiadamente de sus sesiones en el sistema y solamente cortan la llamada, confiando en el sistema para que detecte la desconexión y cierre la sesión.

  Para prevenir este problema, es importante que el equipo de comunicaciones esté diseñado para responder a la pérdida de conexión cuando lo indique el módem (a través de la perdida de la señal portadora, "Carrier Detect").

3.6. Diseño para la administración de red

Si la red de alto desempeño va a proveer un servicio confiable a los usuarios año con año, una administración efectiva de la red es esencial. El diseño de dichos sistemas puede ser complejo, y merece tanta atención como el diseño físico.

La efectividad real de una red de alto desempeño depende de que tan bien se comporte, día tras día, mes con mes y año con año. Un recurso costoso que es central para las operaciones necesita ser cuidado; esto quiere decir, mantener el equipo y asegurar su indiscutible relevancia. Generalmente esto es llamado administración de red y actualmente se ha convertido en administración de servicios [bib04].

Para comenzar, el problema real que se enfrenta en la administración de redes y servicios es el control de la complejidad. Las redes modernas son simplemente muy diversas para ser controladas y son necesarios principios sólidos y el soporte de herramientas poderosas. La capacidad de administración tiene que ser construida como una parte integral del diseño de la red.

En redes de alto desempeño a gran escala, la imagen de la administración inherentemente compleja crece debido a la necesidad de múltiples sistemas de administración, sin embargo la mayoría consta de dos elementos:

- *NOMS (Network Operator Management System).* Plataforma enteramente compatible capaz de proveer soporte operacional a todos los elementos de la red.

- *NUMS (Network User Management System).* Proporciona al usuario final una visión general de la red, generalmente con información de "sólo lectura" obtenida de un NOMS. Esta visión es requerida para todos aquellos con la responsabilidad de operar con aplicación y sistemas finales. La información puede ser integrada con la de los usuarios de sistemas finales para ayudar en la localización de fallas en sistemas finales o en la red.

El objetivo principal deben ser los sistemas diseñados e instalados para permitir la operación diaria de la red, mismos que deben lograr lo siguiente:

- Operación continua.
- Manejo de alarmas.
- Soporte a diagnósticos.
- Creación de estadísticas.
- Control sobre la configuración.

Hay otros aspectos en la administración de redes y servicios que deben ser considerados. Se mencionan solo algunos de ellos:

- *Entrega.* Es el manejo efectivo de las peticiones de servicio, para lo cual se requieren bases de datos efectivas y herramientas de administración de proyectos para soportarlo.

- *Control de inventario.* Tener control de los componentes entregados en la red, asignación de direcciones y la topología de los componentes de interconexión.

- *Auditoria de red.* Herramientas para checar que la red actual coincida con la información recabada de los inventarios y los sistemas de control de configuración.

- *Help desk.* Tener un punto de contacto para manejar las fallas y requerimientos. El equipo de help desk necesita acceso inmediato a los sistemas de administración.

- *Bitácora de fallas y administración.* Un sistema de base de datos se necesita para crear un reporte de fallas. El sistema automáticamente tiene que enviar a los usuarios actualizaciones del estado y escalar las fallas no arregladas dentro de tiempos específicos. El sistema también debe proveer estadísticas en casos de fallas y funcionamiento normal.

Sería bueno que una red bien diseñada, una vez instalada, se mantuviera trabajando. Pero no siempre es el caso, aún en operación estable hay una serie de necesidades que el sistema de administración de red debe satisfacer. Los problemas potenciales que el diseño para la administración de red debe solventar incluyen:

- *Fallas por reacción en cadena.* En donde se necesita saber como una falla en una parte de la red podría afectar la operación total.

- *Congestión por tráfico.* Si varios elementos en la red fallan simultáneamente, la carga del tráfico bloqueado y redireccionado puede ocasionar que el sistema deje de funcionar. Además de la congestión están los mensajes que la red genera para reportar los problemas.

- *Inesperado.* Un red golpeada por eventos inesperados debe ser capaz de ayudarse a sí misma. Debe administrar y redireccionar el tráfico para evitar los sitios con problemas. El sistema también debe reaccionar apropiadamente para duplicar mensajes o verificar mensajes de fuentes cuestionables.

- *Administración centralizada y descentralizada.* La administración centralizada también puede crear un punto central de falla. La administración descentralizada puede ser una fuente de inconsistencia. En una red de alto desempeño, se puede tener cualquiera de los dos elementos, con sus desventajas combinadas. Se debe decidir quien va a ser responsable de administrar cosas como la consistencia en la base de datos, sistemas de respaldo, y actualizaciones a las bases.

- *Estándares de protocolos.* La selección del estándar para la administración de la red puede mejorar su funcionamiento o dificultarlo. Se debe asegurar que todo el sistema opere de la misma forma, en caso contrario, se pueden interpretar mensajes no estandarizados en forma extraña.

- *Potencial de crecimiento.* El sistema de administración se debe adaptar al crecimiento del tráfico y la integración de nuevos nodos y redes. También debe incorporar nueva tecnología y aceptar nuevas características conforme éstas vayan surgiendo.

El diseño de redes LAN Ethernet se ha convertido en la tecnología predominante en la Universidad con el paso de los años. Sin embargo existen otras tecnologías que también han sido instaladas y continúan en funcionamiento como FDDI y ATM, de tal forma que todas operan de manera correcta al momento de interactuar y funcionar como uno de los medios para llevar a cabo las actividades académicas inherentes a la UNAM. Por otro lado, la base de equipo activo instalada también a crecido en una variedad de opciones bastante interesante, encontrándose hubs, switches, routers, equipo inalámbrico, multiplexores, etc.

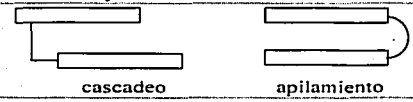
En consecuencia, el conocimiento de todos estos aspectos pasa a primer término cuando se trata del diseño de nuevas redes o remodelaciones de las actuales. Solamente hay que tomar en cuenta que hay que satisfacer nuevas necesidades, acondicionar nuevas instalaciones, evaluar nuevos equipos, probar nuevas tecnologías, integrar distintos servicios en equipos mas robustos, proporcionar flexibilidad para el crecimiento, cambiar probablemente a un nuevo esquema de direccionamiento, etc., sin olvidar seguir manteniendo compatibilidad con todo lo existente. Se reafirma entonces que no existe un kit que se pueda comprar y solucione todos los problemas o satisfaga las necesidades, por el contrario, las soluciones se elaboran paso a paso y con los fundamentos técnicos necesarios para lograrlo.

La mejor forma de reafirmar lo escrito es acercándolo a la realidad, por eso se presentan ejemplos de redes que ya están en funcionamiento y necesitan cambios. Sin embargo, no se va a elaborar un diseño a detalle porque es una labor que requiere mucho tiempo y es muy específica para cada proyecto, sobretodo al evaluar necesidades, platicar con los usuarios, desarrollar la propuesta para cada etapa, etc. Los cambios descritos se enfocan en la parte técnica, por ser el área con un impacto más significativo cuando se trata de mejorar el rendimiento de una red.

Capítulo 4. Tecnologías

Generalmente, los fabricantes incluyen todo un despliegue de tecnologías en los equipos que comercializan, y éstas deben ser evaluadas adecuadamente al momento de tomar una decisión, sobre todo considerando el costo de dichos productos. Aun cuando la diferencia económica entre cada tecnología no sea significativa, es importante conocer la capacidad del equipo adquirido y las posibilidades de éxito que se tendrán al enfrentar las necesidades futuras. No vale la pena invertir en un equipo que represente lo mejor de la tecnología actual si la mayoría de las características que dan el valor al producto no se van a utilizar, aún a largo plazo. El caso contrario también es desventajoso.

Para lograr una comprensión adecuada de las siguientes figuras, es necesario emplear una nomenclatura para identificar cada dispositivo, sobre todo al momento de realizar cambios en las topologías presentadas. Cada equipo deberá tener relacionada una sigla que identifique el tipo de dispositivo, un número de dispositivo y la velocidad a la cual trabaja. También se identificarán las conexiones entre equipos para distinguir un cascadeo de un apilamiento, por lo tanto:

hxy, donde: h = hub x = no. de dispositivo y = velocidad de transmisión (Mb)	sxy, donde: s = switch x = no. de dispositivo y = velocidad de transmisión (Mb)
sax, donde: sa = servidor de aplicación x = no. de dispositivo	

A continuación se presenta una red real en su estado actual con dos características importantes y quizá comunes a la gran mayoría: tiene un bajo, y en algunas secciones nulo, nivel de configuración y cuenta con una gran densidad de usuarios. La figura 24 ilustra una LAN de 10/100Mbps que coexiste con hubs, switches y un switch capa 3 o router.

Caso práctico:

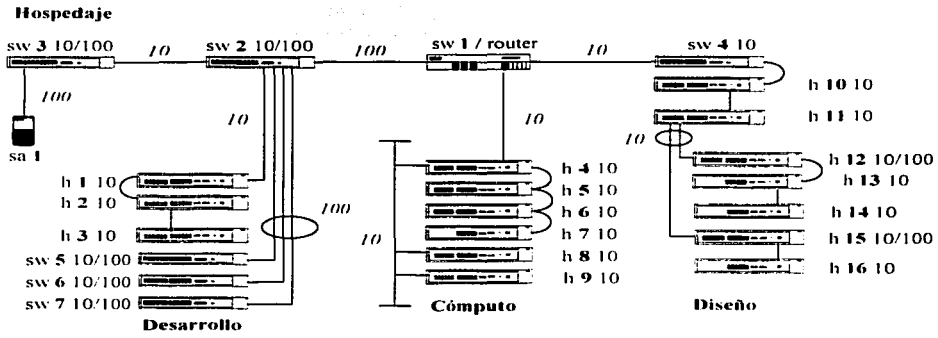


Figura 24. Caso práctico en estado actual

Diseño:
Los switches pueden segmentar hubs para incrementar el rendimiento en LAN compartidas sin cambiar la topología de red, es decir, pueden concentrar el tráfico de varios segmentos Ethernet de 10Mbps al escritorio. Tiene muchos usuarios y necesita hubs apilables, que no fueron adecuadamente provistos y han sido agregados pequeños hubs para soportar los grupos de usuarios, por lo que la plataforma de switches debe ofrecer Fast Ethernet de gran densidad. La figura 25 muestra algunos cambios.

Caso práctico:

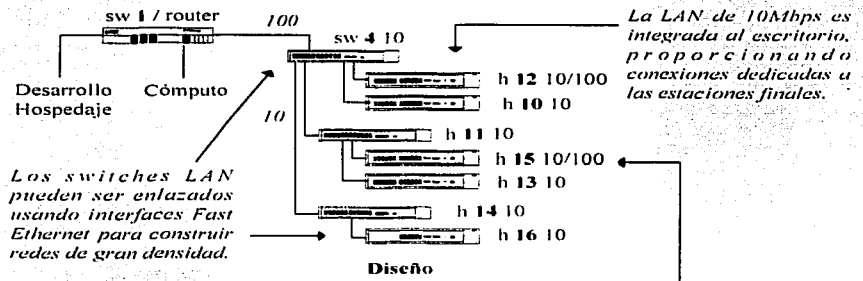


Figura 25. Cambios físicos realizados en el área de diseño

Hospedaje:
Para mejorar el rendimiento cliente/servidor a través de la red, los servidores pueden conectarse directamente a las interfaces Fast Ethernet en los switches LAN. Un ejemplo de esta práctica son las granjas de servidores. Al mismo tiempo, el enlace del switch 2 10/100 hacia el switch 1 / router puede emplear Gigabit Ethernet para obtener velocidades de transmisión mayores. Ver figura 26.

Desarrollo:
Fast Ethernet dedicado es integrado al escritorio, dando un acceso de alto rendimiento a los usuarios de PC y estaciones de trabajo hacia los servidores o Internet. La figura 26 muestra como el sw 2 10/100 puede ser usado para un grupo de usuarios que requieren conexiones de 100Mbps dedicadas. El switch tiene un módulo 100BaseFX que le permite proveer un enlace Fast Ethernet al equipo principal.

Caso práctico:

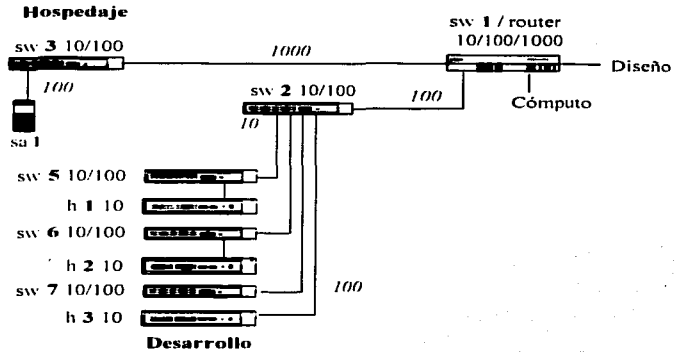


Figura 26. Cambios físicos realizados en el área de desarrollo y hospedaje

Cómputo:
La figura 27 muestra dos formas de proveer una red local. Por un lado ha sido instalada una red 10Base2 en vertical para interconectar los hub. En la derecha, un backbone alternativo se propone utilizando un hub 10BaseFL. El equipo adicional (h 17 10FL) se emplea por dos razones, la primera es que no siempre se cuenta con el dinero suficiente para adquirir un equipo nuevo, la segunda es que en ocasiones existe equipo disponible que puede usarse en este tipo de situaciones. Este caso hace notar que a pesar de que no se tiene el equipo mas reciente, se pueden lograr buenos resultados empleando equipo existente. La clave esta en conocer las consideraciones de diseño adecuadas. Los diseños en los cuales el bus de backbone es reemplazado por un arreglo tipo estrella son comúnmente conocidos como diseños de backbone colapsable.

Caso práctico:

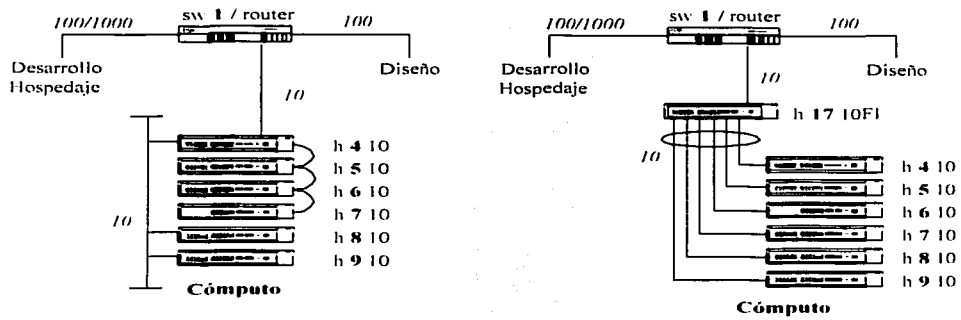


Figura 27. Cambios físicos realizados en el área de cómputo

Resumen caso práctico:

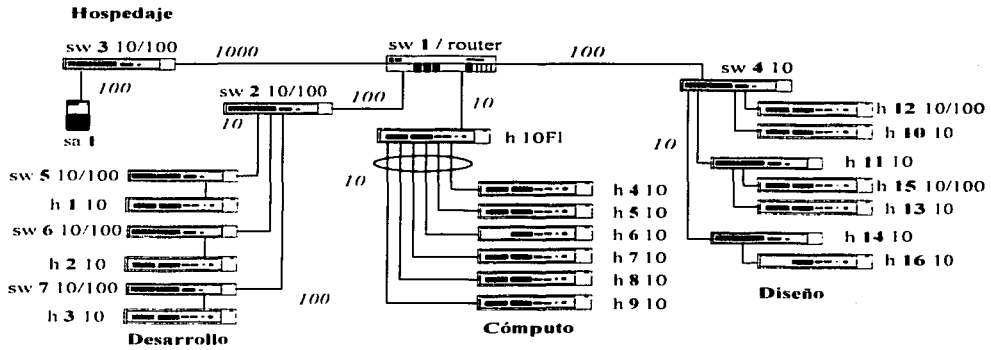


Figura 28. Caso práctico después de cambios físicos realizados en cada una de las áreas

4.1. Configuración inicial

Teniendo en mente la red original, se pueden apreciar los cambios físicos realizados. El siguiente paso es realizar cambios a nivel lógico, modificando la configuración de fábrica. El caso práctico se irá modificando conforme se expongan las tecnologías seleccionadas, mismas que son las más comunes para la mayoría de los equipos utilizados en LAN y LsLAN.

Reenvío de paquetes

Fast forward. Los paquetes son reenviados tan rápido como sea recibida y procesada la dirección destino. Con fast forward, los paquetes toman menos tiempo para ser reenviados, pero todos los paquetes erróneos son propagados en la red porque no hay tiempo para la comprobación de errores.

Fragment free. Los paquetes son reenviados cuando por lo menos 512 bits del paquete son recibidos, lo cual asegura que los fragmentos de colisión no sean propagados en la red. Con fragment free, los paquetes toman menos tiempo para ser reenviados, pero todos los paquetes erróneos excepto los fragmentos son propagados.

Store and forward. En este modo, los paquetes recibidos son almacenados en su totalidad antes de ser reenviados, lo cual asegura que solamente los paquetes buenos sean reenviados a su destino. Con store and forward, los paquetes toman un poco más de tiempo para ser reenviados que con fast forward y fragment free, pero los errores no son propagados [bib04].

Intelligent. El equipo monitorea la cantidad de errores en el tráfico de la red y cambia automáticamente el modo de reenvío. Si el equipo detecta 20 o más errores por segundo, el modo de reenvío es puesto en store and forward hasta que el número de errores por segundo regrese a su valor original. Si el equipo detecta 1 error por segundo, el modo de reenvío es puesto en fast forward.

Modos de transmisión

Half duplex. Permite que los paquetes sean transmitidos y recibidos, pero no simultáneamente. Este es el modo Ethernet predeterminado.

Full duplex. Permite que los paquetes sean transmitidos y recibidos simultáneamente y, en efecto, duplica el potencial de conexión.

Control de flujo

El control de flujo es un mecanismo para el control de congestiones. Las congestiones son causadas por uno o más dispositivos enviando tráfico a un puerto ya saturado. El control de flujo evita la perdida de paquetes e impide que los dispositivos continúen generando más paquetes hasta que el periodo de congestión termine.

Priorización de tráfico

Hay equipos que soportan IEEE 802.1P priorización de tráfico, lo cual permite que los datos asignados con alta prioridad sean reenviados a través del equipo sin ser obstruidos por otros datos. El sistema trabaja usando múltiples colas de tráfico presentes en el hardware del equipo, es decir, el tráfico de alta prioridad es reenviado a una cola diferente, y siempre se le da preferencia sobre el demás tráfico. La priorización de tráfico puede ser sumamente útil para aplicaciones críticas que requieren una alta calidad de servicio (Class of Service, CoS) de la red.

Address learning

Esta característica de seguridad protege contra usuarios no autorizados que se quieran conectar a dispositivos en la red. Cuando es activado en un puerto, éste entra en el modo de aprendizaje para una dirección. En este modo:

- Remueve todas las direcciones MAC almacenadas para el puerto en la matriz de conmutación del equipo.
- Aprende la dirección del primer paquete que recibe en el puerto.
- Define la dirección como una entrada permanente.

Matriz de conmutación

La matriz de conmutación de un equipo es usada para determinar si un paquete debe ser reenviado, y en tal caso, cual puerto debe transmitir el paquete. La matriz de conmutación contiene una lista de entradas, cada una con tres campos:

- La dirección MAC de cada estación final que envíe paquetes al equipo.
- El puerto del equipo que recibe paquetes de la estación final.
- El identificador local de la VLAN a la cual pertenece el sistema final.

Las entradas en la matriz de conmutación pueden tener tres estados:

- *Aprendida*. El equipo ha puesto la entrada en la matriz de conmutación cuando el paquete fue recibido de la estación final.
  - Las entradas aprendidas son removidas (caducadas) de la matriz de conmutación si no se reciben paquetes de la estación final dentro de un cierto periodo de tiempo (tiempo de vida). Esto evita que la matriz de conmutación se llene con datos obsoletos asegurando que cuando una estación final es removida de la red, su entrada es también removida de la matriz de conmutación.
  - Las entradas aprendidas también son removidas de la matriz de conmutación si el equipo es reinicializado o desconectado de la toma eléctrica.
- *Aprendida sin tiempo de vida*. Si el tiempo de vida es puesto en 0 segundos, todas las entradas aprendidas en la matriz de conmutación se convierten en entradas sin tiempo de vida. Esto significa que no caducan, pero se remueven de la matriz de conmutación si el equipo es reinicializado o desconectado de la toma eléctrica.

- *Permanente.* La entrada es puesta en la matriz de conmutación de forma manual. Las entradas permanentes no son removidas del equipo a menos que sea hecho manualmente o el equipo sea reinicializado.

Caso práctico:
Podemos entonces aplicar el modo intelligent a toda la red presentada. Sin embargo, en las áreas en las cuales se ha puesto un switch como equipo de distribución, la cantidad de colisiones disminuye de forma considerable, debido a su propio funcionamiento, por lo que podría ser una práctica segura dejar una configuración tipo fast forward. La desventaja es que los switches tiene conectados hubs y en tales condiciones es recomendable el tipo intelligent.

Para comunicarse efectivamente, ambos extremos del enlace deben usar el mismo modo de transmisión. Si el enlace usa conexión autonegociada, esto se hace automáticamente. Si el enlace usa una conexión no autonegociada, ambos extremos deben ser configurados manualmente. El proceso de negociación permite a los dispositivos en cada extremo de un enlace de red intercambiar información automáticamente acerca de sus capacidades y llevar a cabo la configuración necesaria para operar conjuntamente a su mayor capacidad. Por ejemplo, la autonegociación puede determinar si un hub 100Mbps está conectado a un adaptador 10/100Mbps y después ajustar el modo de operación. También se provee una función paralela que permite reconocer half/full duplex, aún si uno de los dispositivos conectados no ofrece capacidades de autonegociación.

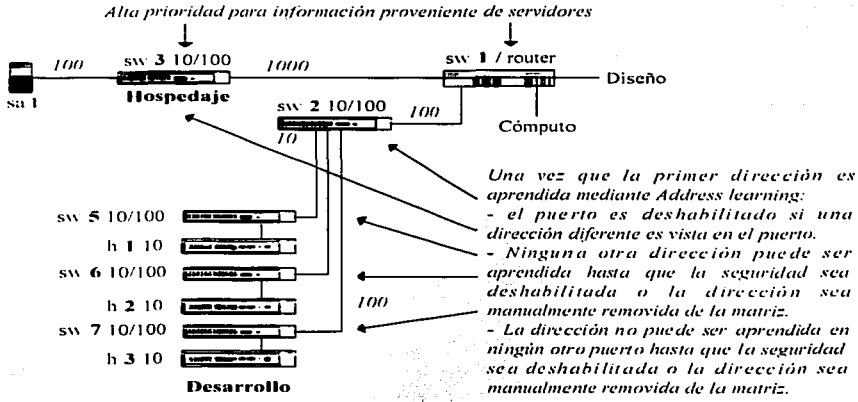


Figura 29. Caso práctico con las primeras modificaciones en la configuración de los equipos (reenvio, modo de transmisión y address learning)

Enlaces de respaldo

Esta característica permite proteger los enlaces críticos y evitar periodos sin servicio si dichos enlaces fallan. Los enlaces de respaldo son un método simple para crear redundancia que permita una reacción instantánea a fallas. Los enlaces de respaldo son rápidos de activar, se tiene pleno control sobre su configuración y el puerto del extremo remoto del enlace no necesita tener soportada esta característica.

Un enlace de respaldo está conformado de un par conteniendo un enlace principal y un enlace de respaldo. Si el enlace principal de comunicación falla, el enlace duplicado inmediata y automáticamente toma la carga de trabajo del enlace principal.

Cuando se configuran enlaces de respaldo, se debe observar lo siguiente:

- Los pares de un enlace de respaldo no pueden ser establecidos si el equipo usa el protocolo Spanning Tree
- Los pares de un enlace de respaldo sólo pueden configurarse si pertenecen a la misma VLAN y utilizan el mismo sistema VLAN tagging.

Port trunk

Son conexiones que permiten a los dispositivos comunicarse usando hasta cuatro enlaces en paralelo. Proveen dos beneficios:

- Pueden duplicar, triplicar o cuadruplicar la capacidad de una conexión.
- Pueden proveer redundancia. Si un enlace falla, los otros comparten el tráfico de ese enlace.

Cuando se configura un port trunk, se debe notar lo siguiente:

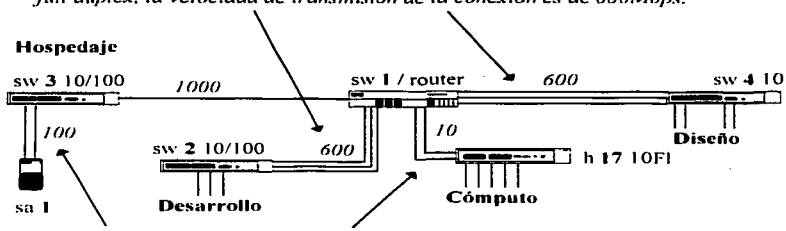
- Los puertos en ambos extremos de la conexión deben ser configurados como port trunk.
- Los puertos solamente pueden pertenecer a un port trunk, y deben ser del mismo equipo.
- Si puertos con diferente velocidad son ubicados en el mismo port trunk, los enlaces más rápidos cargan con el tráfico. Los enlaces con menor capacidad solamente cargan con el tráfico si los primeros fallan.

Cuando se utiliza port trunk, se debe notar lo siguiente:

- Para recabar estadísticas acerca del port trunk, se deben agregan las estadísticas de cada puerto.
- Para deshabilitar un enlace en el port trunk, se debe remover la conexión y después deshabilitar ambos puertos del enlace. De esta manera, el tráfico destinado para ese enlace es distribuido a los otros enlaces en el port trunk. Si solamente se remueve la conexión en el port trunk, el tráfico continúa reenviándose a ese puerto por el extremo remoto. Esto significa que una gran cantidad de tráfico puede perderse.

Caso práctico:

Los requerimientos de ancho de banda pueden situar demandas significativas en la red. Port trunk permite que varios puertos (generalmente hasta cuatro) sean unidos y vistos lógicamente como una gran tubería. Si tres puertos en las dos unidades son configurados como 100Base-TX y están operando en modo full duplex, la velocidad de transmisión de la conexión es de 600Mbps.



Cuando se configuran enlaces de respaldo, se debe observar lo siguiente:
- Un enlace de respaldo solamente se define en un extremo de la conexión.
- Ninguno de los puertos tiene algún esquema de seguridad.
- Ninguno de los puertos es parte de un port trunk.
- Ninguno de los puertos pertenece a otro sistema de enlace de respaldo.

Figura 30. Caso práctico habilitando enlaces de respaldo y port trunk

4.2. VLAN

Una VLAN es un grupo flexible de dispositivos que pueden ser situados en cualquier parte de una red, pero se comunican como si estuvieran en el mismo segmento físico. Con las VLAN, se puede segmentar la red sin estar limitado por las conexiones físicas.

El principal beneficio de las VLAN es que proveen un sistema de segmentación de la red que es más flexible que cualquier red tradicional. Usar VLAN también provee otros tres beneficios:

- *Facilita el cambio y movimiento de dispositivos en redes IP.* Con redes IP tradicionales, los administradores de red utilizan mucho de su tiempo lidiando con movimientos y cambios. Si los usuarios se mueven a una subred IP diferente, la dirección IP de cada estación final debe ser actualizada manualmente. Con una VLAN establecida, si una estación final en la VLAN1 es movida a un puerto en otra parte de la red, solo se necesita especificar que el nuevo puerto reenvíe tráfico de la VLAN1.

- *Provee seguridad extra.* Los dispositivos dentro de una VLAN solamente pueden comunicarse directamente con dispositivos en la misma VLAN. Si un dispositivo en la VLAN1 necesita comunicarse con dispositivos en la VLAN2, el tráfico necesita pasar a través de un router o un switch capa 3.

- *Ayuda a controlar el tráfico broadcast.* Con redes tradicionales, la congestión puede ser causada por tráfico broadcast que es dirigido a todos los dispositivos de la red sin importar si lo requieren o no. Las VLAN incrementan la eficiencia de la red porque cada una puede ser establecida para contener solo aquellos dispositivos que necesiten comunicarse entre ellos.

Generalmente los equipos proveen las siguientes características:

- Soporte para un determinado número de VLAN usando el estándar IEEE 802.1Q, mismo que permite a cada puerto del equipo:
  - Ser situado en cualquier VLAN definida en el equipo.
  - Ser situado en varias VLAN definidas en el equipo.
  - Usar IEEE 802.1Q learning. Un sistema que permite al equipo aprender los requisitos VLAN de las estaciones finales conectadas a cada puerto, y situar los puertos relevantes en esas VLAN automáticamente.
  - Reenviar tráfico de VLAN que son desconocidas para el equipo.

- El estándar requiere que se defina la siguiente información acerca de cada VLAN:
  - *Nombre VLAN.* Es un nombre descriptivo para la VLAN.
  - *IEEE 802.1Q VLAN ID.* Es usado para identificar la VLAN si se utiliza IEEE 802.1Q tagging a través de la red.
  - *ID local.* Es usado para identificar la VLAN dentro del equipo.

4.2.1. VLAN no etiquetadas y etiquetadas

Cuando se establecen VLAN se necesita entender cuando usar VLAN sin etiquetar o etiquetadas. Si un puerto está en una sóla VLAN éste puede ser sin etiquetar pero si el puerto necesita ser miembro de múltiples VLAN debe ser etiquetado.

El estándar IEEE 802.1Q define como operan las VLAN dentro de una red conmutada de arquitectura abierta. Un paquete acorde a IEEE 802.1Q transporta información adicional que permite al equipo determinar a que VLAN pertenece el puerto. Esta trama es conocida como etiquetada.

Para transportar múltiples VLAN a través de un sólo enlace físico, cada paquete debe estar etiquetado con un identificador VLAN para que el equipo pueda saber que paquetes pertenecen a que VLAN. Los routers

interconectan VLAN, así que ellos también deben entender el etiquetado IEEE 802.1Q, para que no se conviertan en cuellos de botella para el tráfico entre VLAN.

4.2.2. IEEE 802.1Q learning

Si una estación final soporta IEEE 802.1, ésta puede ser configurada para informar a la red que está para recibir tráfico de ciertas VLAN. Si el equipo cuenta con la misma capacidad, se puede hacer lo siguiente:

- Automáticamente situar la estación final en esas VLAN.
- Automáticamente asegurar que el tráfico VLAN requerido pueda siempre alcanzar a la estación final en cualquier parte de la red.

El sistema funciona de la siguiente manera:

1. La estación final configurada con IEEE 802.1Q envía un paquete a toda la red con una dirección multicast conocida. Este paquete declara que la estación final está lista para recibir tráfico de las VLAN especificadas.

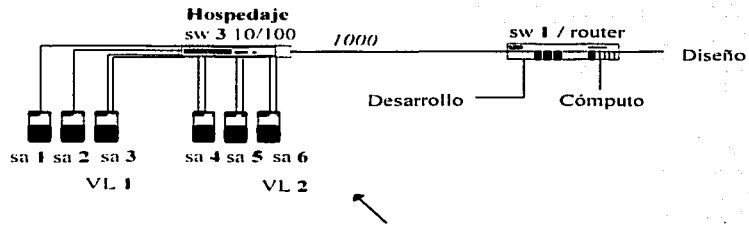
2. Cuando el paquete llega a un puerto del equipo con IEEE 802.1Q learning activado, el equipo sitúa el puerto en las VLAN especificadas y luego reenvía el paquete a todos los demás puertos.

3. Cuando el paquete llega a otro equipo con IEEE 802.1Q learning activado, también sitúa el puerto receptor en las VLAN especificadas y reenvía el paquete a todos los demás puertos. De esta forma la información VLAN es propagada a través de la red, y el tráfico VLAN requerido siempre puede alcanzar a la estación final sin importar su ubicación en la red.

4.2.3. IEEE 802.1Q etiquetas desconocidas

El estándar IEEE 802.1Q permite hasta 4,094 VLAN definidas en una red. Si la red contiene estaciones finales que soportan IEEE 802.1Q, el equipo puede necesitar reenviar tráfico que use etiquetas IEEE 802.1Q desconocidas. Este tráfico es automáticamente reenviado si se cuenta con IEEE 802.1Q learning activado.

Caso práctico:



La vlan más simple opera en una red pequeña usando un solo switch. En esta red no se requiere pasar el tráfico vlan a través de un enlace. Se ilustra un solo switch conectado a estaciones finales y servidores usando conexiones no etiquetadas. Tres puertos del switch pertenecen a la vlan1, y tres puertos pertenecen a la vlan2. vlan1 y vlan2 están completamente separadas y no pueden comunicarse entre ellas.

Figura 31. Caso práctico empleando una VLAN para el área de hospedaje

Caso práctico:

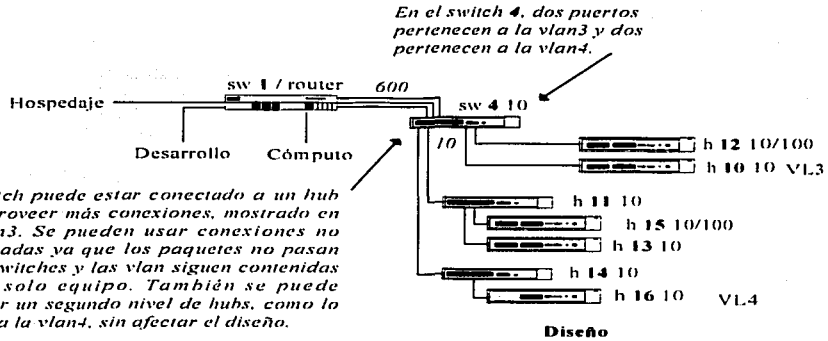


Figura 32. Caso práctico empleando una VLAN para crear dos grupos de equipos en el área de diseño

Caso práctico:

Cada switch tiene estaciones finales conectadas a las vlan creadas y ha sido agregado un servidor en cada vlan. Los servidores en las vlan 3, 4 y 5 necesitan conectarse a los servidores colocados en la vlan1 del switch de hospedaje. También es necesario especificar que algunos enlaces deben pertenecer a otras vlan, de lo contrario podrían quedar incomunicadas una o todas las redes.

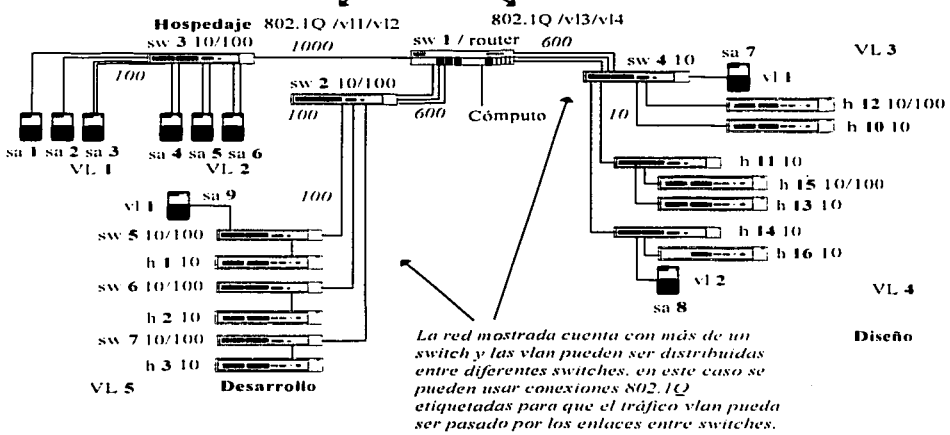


Figura 33. Caso práctico en el cual se extiende el uso de VLAN de tal forma que es posible mezclar físicamente los equipos mientras se mantienen agrupados lógicamente

Caso práctico:

Si se tiene estaciones finales que soportan IEEE 802.1Q y dispositivos de red que tienen 802.1Q learning activado, cada estación informa a la red que está disponible para recibir tráfico de ciertas vlan, y los dispositivos de red automáticamente colocan la estación final en esas vlan. Además, los enlaces entre los dispositivos de red son automáticamente configurados para reenviar tráfico que contenga etiquetas 802.1Q desconocidas.

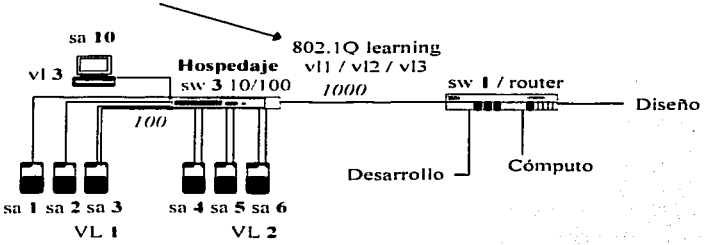


Figura 34. Caso práctico con IEEE 802.1Q learning activado para el área de hospedaje

4.3. FastIP

Es un sistema que permite usar el estándar IEEE 802.1Q para reducir la carga en los dispositivos de ruteo cuando las VLAN son implementadas en la red.

Los dispositivos en diferentes VLAN solamente pueden comunicarse usando un dispositivo de ruteo; si hay una gran cantidad de tráfico entre VLAN, el router puede saturarse y afectar el rendimiento de la red. FastIP permite a las estaciones finales y switches encontrar atajos seguros para el tráfico entre VLAN. Cuando se usa FastIP, se debe tener un dispositivo de ruteo en la red (switch capa3 o router).

FastIp funciona de la siguiente manera:

1. Si una estación final A soporta FastIP, ésta determina que paquetes serán enviados a una estación final local (en la misma VLAN) o a una estación remota (en otra VLAN).

2. Si la estación final A esta por enviar un paquete a la estación final remota B, ésta envía un paquete NHRP especial (Next Hop Resolution Protocol) a la estación final B. El paquete contiene la dirección MAC y detalles de la membresía VLAN a la que pertenece la estación final A.

3. El paquete NHRP pasa a través del switch hacia el dispositivo router, y de regreso a un switch hasta la estación final B.

4. Si la estación final B soporta FastIP, ésta graba la dirección MAC y membresía VLAN de la estación final A.

5. La estación final B envía un paquete NHRP con sus propios detalles de regreso a la estación final A. El paquete, sin embargo, es enviado directamente a través de los switches y no a través de los routers. Para hacer esto, la estación final B especifica lo siguiente:

- El paquete es enviado a las VLAN que la estación final A puede recibir.
- El paquete tiene la dirección MAC destino de la estación final A.

6. La estación final A recibe el paquete NHRP de la estación final B y graba la dirección MAC y la membresía VLAN de la estación B.

7. La estación final A envía la información a la estación final B directamente a través de los switches. Para hacer esto, la estación final A especifica lo siguiente:
   - El paquete es enviado a las VLAN que la estación final B puede recibir.
   - El paquete tiene la dirección MAC destino de la estación final B.

FastIp y matriz de conmutación

Por omisión, la matriz de conmutación de un switch es dividida por VLAN, cada una con un área independiente. Con este sistema, la matriz de conmutación puede almacenar una entrada para un dispositivo en varias VLAN al mismo tiempo, y la entrada para una VLAN en particular puede ser almacenada en diferentes puertos. Como ejemplo, la tabla 7.1 ilustra la matriz de conmutación de un switch almacenando una entrada para una estación final A en las VLAN 1, 2 y 3, y las entradas son almacenadas en el puerto 1.

		VLAN		
		1	2	3
Puerto	1	A	A	A
	2			
	3			

Tabla 7.1. Matriz de conmutación almacenando una entrada

La tabla 7.2 ilustra la matriz de conmutación almacenando una entrada para la estación final A en las VLAN 1, 2 y 3. Aquí, la entrada de la VLAN1 está en el puerto 1, la entrada de la VLAN2 está en el puerto 2 y la entrada de la VLAN3 está en el puerto 3.

		VLAN		
		1	2	3
Puerto	1	A		
	2		A	
	3			A

Tabla 7.2. Matriz de conmutación almacenando una entrada en varios puertos

Cuando FastIP es usado por el switch, la matriz de conmutación ya no puede ser dividida por VLAN, ésta debe ser compartida por todas las VLAN:

Caso práctico:

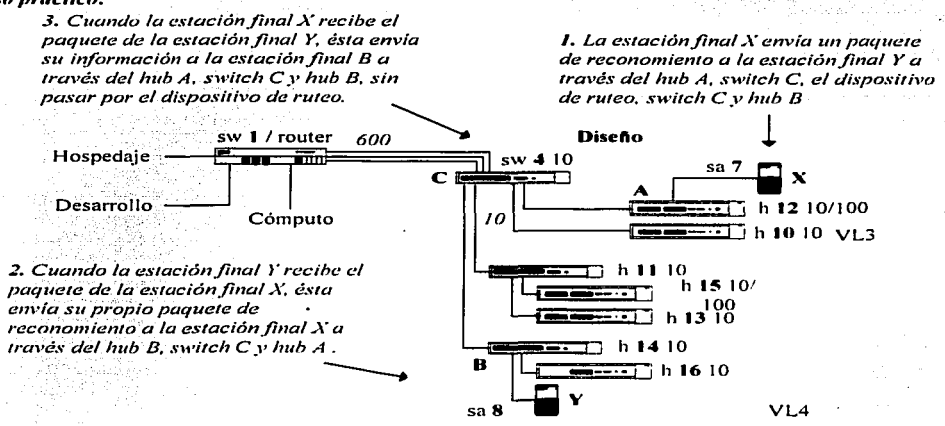


Figura 35. Caso práctico utilizando FastIP en el área de diseño

4.4. Multicast filtering y Spanning tree

Un multicast es un paquete que es enviado a un grupo de estaciones finales en una LAN, o VLAN, que pertenecen a un grupo multicast. Si la red es configurada correctamente, un multicast también puede ser enviado a una estación final si ésta se ha unido al grupo en cuestión. Un uso típico de multicast es videoconferencia, en donde los altos volúmenes de tráfico necesitan ser enviados a varias estaciones finales simultáneamente, pero enviar el tráfico a todas las estaciones finales podría reducir seriamente el rendimiento de la red.

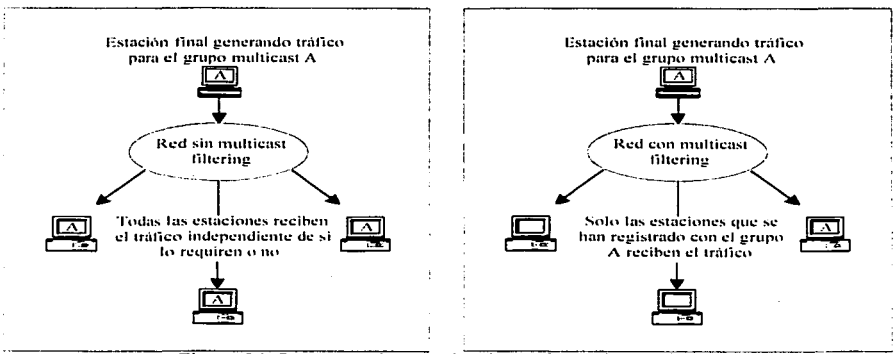


Figura 36. Demostración del funcionamiento de multicast

Existen dos sistemas de multicast filtering:

- IEEE 802.1P.
- IGMP (Internet Group Management Protocol).

4.4.1. IEEE 802.1P multicast filtering

El estándar IEEE 802.1P define un sistema que permite a los dispositivos de red registrar las estaciones finales en grupos multicast.

IEEE 802.1P multicast filtering trabaja de la siguiente manera:

1. Si una estación final IEEE 802.1P quiere recibir tráfico de un grupo multicast, envía un paquete unión con una dirección multicast conocida para declarar que desea unirse al grupo.
2. Cuando el paquete unión arriba a un puerto de un switch con IEEE 802.1P multicast learning activado, el switch especifica que el puerto está listo para reenviar tráfico del grupo multicast y después envía un paquete similar a los otros puertos.
3. Cuando aparece tráfico para el grupo multicast en la red, el switch solo reenvía el tráfico a los puertos que recibieron el paquete unión.

4.4.2. IGMP multicast filtering

IGMP es un sistema que puede ser usado en todas las LAN o VLAN que contengan un router IP y otros dispositivos de red que soporten IP, para registrar estaciones finales en un grupo multicast.

IGMP multicast filtering trabaja de la siguiente forma:

1. El router IP periódicamente envía paquetes *query* a todas las estaciones finales en las LAN o VLAN que tenga conectadas.
   Si la red tiene más de un router IP, el que tenga la dirección IP más baja se convierte en el interrogador. Si la red pierde sus conexiones al router IP, el switch con la dirección IP más baja toma su lugar. Si esto ocurre, multicast filtering solamente puede ocurrir en la VLAN omisión.

2. Cuando una estación final IP recibe un paquete *query*, ésta envía un paquete *report* de vuelta que identifica al grupo multicast al cual la estación final desea unirse.

3. Cuando el paquete *report* arriba a un puerto de un switch con IGMP multicast learning activado, el switch especifica que el puerto puede reenviar tráfico para el grupo multicast y luego reenvía el paquete al router.

4. Cuando el router recibe el paquete *report*, éste registra que la LAN o VLAN requiere tráfico para los grupos multicast.

5. Cuando el router reenvía tráfico del grupo multicast a la LAN o VLAN, el switch solo reenvía tráfico a los puertos que recibieron un paquete *report*.

4.4.3. Spanning tree

Es un sistema que hace a la red más resistente a fallas y también provee protección contra los *loops*, una de las mayores causas de tormentas de broadcast.

STP (*Spanning Tree Protocol*) permite implementar caminos paralelos para el tráfico de la red y usa un proceso de detección de loops para:

- Descubrir la eficiencia de cada camino.

- Activar el camino más eficiente.
- Deshabilitar los caminos menos eficientes.
- Activar uno de los enlaces menos eficientes si el camino más eficiente falla.

Caso práctico:

1. *La red contiene tres segmentos LAN separados por tres switches. En esta configuración, cada segmento puede comunicarse con los demás usando dos caminos. Sin STP, se crean loops que ocasionan que la red se sobrecargue; sin embargo, STP permite tener esta configuración porque detecta caminos duplicados y evita, o bloquea, que uno de ellos reenvíe tráfico.*

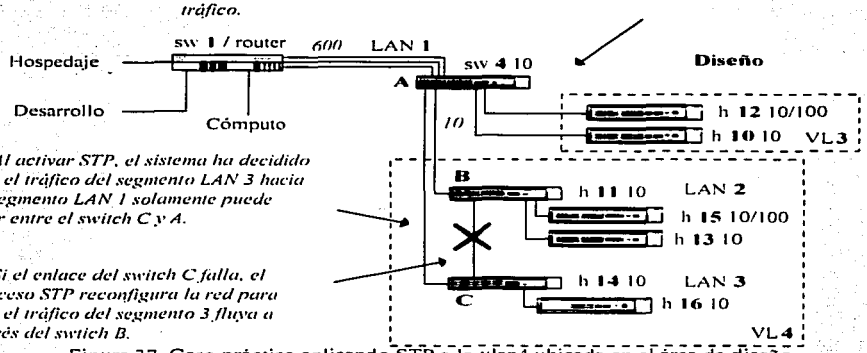


Figura 37. Caso práctico aplicando STP a la vlan4 ubicada en el área de diseño

Requisitos STP

Antes de poder configurar la red, el sistema STP requiere lo siguiente:

- Comunicación entre todos los switches.
- Cada switch con un identificador de switch. Establece el switch que actúa como el punto de referencia central, o switch raíz, para el sistema STP —entre más bajo sea el identificador del switch más posibilidades hay de convertirse en switch raíz. El identificador de switch es calculado usando la dirección MAC y una prioridad definida para el switch (ej. 32768).
- Cada puerto con un costo. Especifica la eficiencia de cada enlace, usualmente determinado por el ancho de banda del enlace —entre más alto el costo, menos eficiente el enlace. La tabla 8 muestra ejemplos de costos para diferentes tipos de puertos.

Tipo de puerto	Duplex	Costo
1000BASE-SX	Full	4
Port trunk 100BASE-TX/100BASE-FX	Full/Half	15
100BASE-TX/100BASE-FX	Full	18
	Half	19
Port trunk 10BASE-T	Full/Half	90
10BASE-T	Full	95
10BASE-T	Half	100

Tabla 8. Costo especificado para los puertos más utilizados

Para mejorar el entendimiento, se presenta el ejemplo de la figura 38.

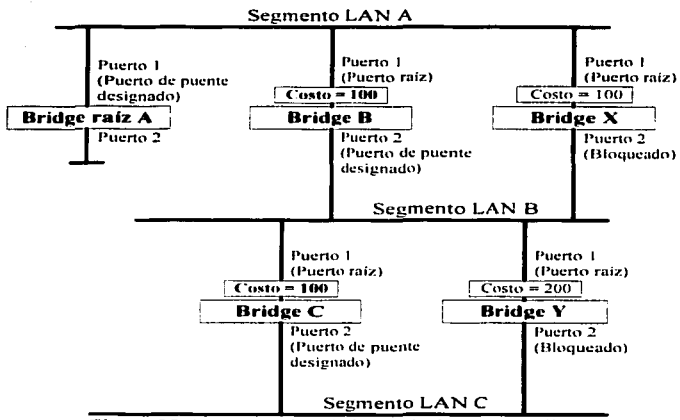


Figura 38. Demostración de la teoría de costos aplicada

- *El bridge A tiene el identificador de bridge más bajo en la red, y ha sido seleccionado como bridge raíz.*
- *Debido a que el bridge A es el bridge raíz, es también el bridge designado para el segmento LAN A. El puerto 1 en el bridge A es seleccionado como el puerto designado del bridge para el segmento A.*
- *El puerto 1 en los bridges B, C, X y Y se ha definido como puertos raíz por ser los más cercanos al bridge raíz.*
- *Los bridges B y X ofrecen el mismo costo para el camino raíz en el segmento LAN B, sin embargo, el bridge B ha sido seleccionado como el bridge designado para el segmento porque éste tiene un identificador de bridge menor. El puerto 2 en el bridge B es seleccionado como el puerto del bridge seleccionado para el segmento LAN B.*
- *El bridge C ha sido seleccionado como el bridge designado para el segmento LAN B, porque éste ofrece el menor costo en el camino raíz para el segmento C —el camino a través del bridge C y B cuesta 200 (C-B=100, B-A=100), el camino a través de los bridges Y y B cuesta 300 (C-B=200, B-A=100). El puerto 2 en el bridge C es seleccionado como el puerto del bridge designado para el segmento C.*

Cálculo STP

La primera etapa en el proceso STP es la que se refiere al cálculo. Durante ésta, el sistema va a determinar:

- La identidad del equipo que va a ser el equipo raíz —el punto de referencia central desde el cual la red es configurada.
- Los costos del camino raíz para cada equipo —esto es, el costo de los caminos de cada equipo hacia el equipo raíz.
- La identidad del puerto de cada equipo que va a ser el puerto raíz —el que está conectado al equipo raíz usando el camino más eficiente, esto es, el que tiene el camino raíz con menor costo. Note que el equipo raíz no tiene puerto raíz.
- La identidad del equipo que va a ser el equipo designado de cada segmento LAN —el que tiene el camino raíz con menor costo del segmento. Note que si varios equipos tienen el mismo costo para el camino raíz, el que tenga el menor identificador de equipo se convierte en el equipo designado.

Todo el tráfico destinado para pasar en la dirección del equipo raíz fluye a través del equipo designado. El puerto en este equipo que se conecta a los segmentos es el puerto designado del equipo.

Configuración STP

Después de que todos los equipos en la red han acordado en la identidad del equipo raíz, y han establecido los demás parámetros relevantes, cada equipo es configurado para reenviar tráfico solamente entre su puerto raíz y el puerto del equipo designado para el segmento de red respectivo. Todos los demás puertos son deshabilitados para recibir y reenviar tráfico.

Reconfiguración STP

Una vez que la topología de red es estable, todos los equipos están preparados para escuchar BPDU's *Hello* especiales del equipo raíz a intervalos regulares. Si un equipo no recibe un BPDU *Hello* después de cierto intervalo, el equipo asume que el equipo raíz, o un enlace entre él mismo y el equipo raíz, se ha descompuesto. El equipo entonces reconfigura la red para asimilar el cambio. En el caso en que se esté trabajando con VLAN, todos los puertos del equipo designado y los puertos raíz deben pertenecer a la misma VLAN.

STP determina cual es el camino más eficiente entre cada segmento y una referencia especial asignada se apunta en la red. Una vez que se ha determinado el camino más eficiente, todos los demás caminos son deshabilitados. Así que, en el caso anterior, STP inicialmente decidió que el camino a través del switch C fue el camino más eficiente y bloqueó el camino a través del switch B. Después de la falla del switch C, STP reevaluó la situación y abrió el camino a través del switch B.

STP con múltiples VLAN

Un switch puede tomar en cuenta las VLAN cuando calcula información STP. Los cálculos solamente son realizados sobre la base de conexiones duplicadas. Por esta razón, algunas configuraciones de red pueden resultar en VLAN siendo subdivididas en un grupo de conexiones aisladas por el sistema STP.

Por ejemplo, la figura 39 muestra una red conteniendo la VLAN 1 y 2. Están conectadas usando el enlace etiquetado IEEE 802.1Q entre el switch B y el switch C. Por omisión, este enlace tiene un costo de 100 y es automáticamente bloqueado porque la otra conexión switch a switch tiene un costo de 36 (18+18). Esto significa que ambas VLAN son subdivididas, la VLAN 1 en los switches A y B no puede comunicarse con la VLAN 1 en el switch C, y la VLAN 2 en los switches A y C no puede comunicarse con la VLAN 2 en el switch B.

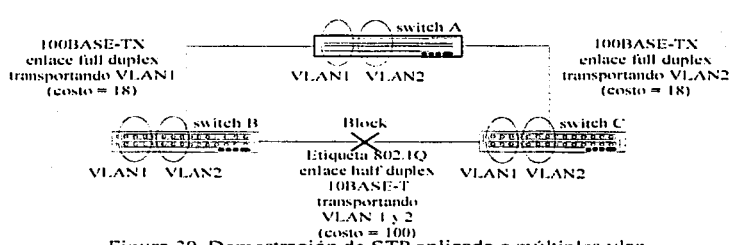


Figura 39. Demostración de STP aplicado a múltiples vlan

Para evitar cualquier subdivisión de VLAN, se recomienda que todas las interconexiones entre switches se conviertan en miembros de todas las VLAN IEEE 802.1Q disponibles para asegurar la conectividad en todo

momento. Por ejemplo, las conexiones entre los switches A y B y los switches A y C deberían estar etiquetadas con IEEE 802.1Q y transportando las VLAN 1 y 2.

4.5. Administración

Existen cuatro métodos de administración:

- *Administración por interfaz web.* Conjunto interno de páginas que permiten la administración del equipo con cualquier navegador con Java activado. Se puede acceder a la interfaz web usando:
  - Una estación de trabajo conectada a la red.
  - Una estación de trabajo conectada al puerto de consola, corriendo el protocolo SLIP (Serial Line Internet Protocol.
- *Administración por interfaz de línea de comando.* Interfaz de línea de comando en el equipo que permite una administración limitada. Se puede acceder a esta interfaz usando:
  - Una terminal o emulador de terminal conectado a la red usando Telnet.
  - Una terminal o emulador de terminal conectado al puerto de consola del equipo.
- *Administración RMON.* Administración descentralizada hacia cualquier equipo. Básicamente consiste de un agente remoto y un sistema central, siendo necesarios ambos para recabar información de los equipos conectados a la red.
- *Administración SNMP.* Administración centralizada de equipos usando cualquier aplicación de administración corriendo SNMP (Simple Network Management Protocol), como 3com Transcend, SUN Net Manager o HP Openview.

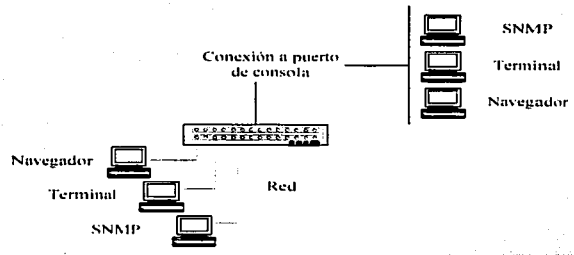


Figura 40. Métodos de administración

4.5.1. RMON

RMON (Remote Monitoring) es un estándar definido por el IETF que permite monitorear las redes LAN o VLAN remotamente [bib04]. Estándar propuesto en 1992 como RFC 1271 (para Ethernet) y finalmente aceptado en 1995 como RFC1757.

El software constantemente crea estadísticas acerca de los segmentos de red conectados a sus puertos. Si se tiene una estación de trabajo con una aplicación de administración RMON, el equipo puede transferir las estadísticas cuando se le solicite o de acuerdo a actividades programadas. Una configuración típica RMON consiste de dos componentes:

- *RMON remoto*. Un dispositivo o agente software inteligente controlado remotamente que continuamente recolecta estadísticas acerca de un segmento LAN o VLAN, y transfiere la información a una estación de administración bajo demanda o cuando se lleve a cabo una calendarización.

- *Estación de administración*. Se comunica con el RMON remoto y recolecta las estadísticas de éste. La estación de trabajo no tiene que estar en la misma red que el RMON remoto y puede administrarlo en conexiones dedicadas o no.

4.5.1.1. Grupos RMON

El IETF define nueve grupos de estadísticas Ethernet RMON. A continuación se describen estos grupos:

Statistics

Provee estadísticas de tráfico y errores medidos por el RMON remoto para cada interfaz monitoreada en el dispositivo. Sus elementos son: paquetes descartados, paquetes enviados, bytes enviados (octetos), paquetes broadcast, paquetes multicast, errores CRC, cortos, gigantes, fragmentos, jabbers, colisiones y contadores para paquetes en los rangos 64-128, 128-256, 256-512, 512-1024 y 1024-1518 bytes.

La información del grupo de estadísticas es usada para detectar cambios en los patrones de tráfico y errores en áreas críticas de la red.

History

Provee referencias históricas del rendimiento de la red tomando muestras periódicas de los contadores proporcionados por el grupo Statistics. Sus elementos son: periodo de muestreo, número de muestras y elemento muestreado.

El grupo es útil para analizar los patrones de tráfico y cambios en los segmentos LAN o VLAN, y para establecer los parámetros de operación normal de la red.

Alarms

Provee un mecanismo para establecer fronteras e intervalos de muestreo para generar eventos en cualquier variable en el RMON remoto. Sus elementos son: tabla de alarmas (requiere la activación del grupo Events), tipo de alarma, intervalo, límite superior y límite inferior.

Las alarmas son usadas para informarse de los problemas en el rendimiento de la red y activar respuestas automáticas a través de los grupos de eventos.

Hosts

Especifica una tabla con estadísticas de tráfico y errores para cada estación final en un segmento LAN o VLAN. Sus elementos son: dirección de nodo, paquetes enviados y recibidos, octetos enviados y recibidos, así como broadcast, multicast y paquetes erróneos enviados.

El grupo proporciona una lista de todos los usuarios que han transmitido a través de la red. El siguiente grupo requiere la implementación del grupo Hosts.

Hosts Top N

Este grupo extiende la tabla de Hosts proporcionando estadísticas indexadas de usuarios, como los 20 usuarios que envían más paquetes o una lista ordenada acorde a los errores que enviaron las últimas 24 horas. Sus elementos son: Statistics, host(s), inicio y fin de los periodos de muestreo, razón y duración.

Matrix

Muestra la cantidad de tráfico y número de errores entre dos dispositivos de red en un segmento LAN o VLAN. Para cada par, el grupo Matrix crea una entrada en su tabla. Sus elementos son: dirección origen y destino, contadores para el número de paquetes, número de octetos y paquetes erróneos entre los dispositivos.

Matrix ayuda a examinar las estadísticas de la red en mayor detalle para descubrir, por ejemplo, quien habla con quien o si una PC en particular está produciendo más errores cuando se comunica con su servidor de archivos. Combinado con Hosts Top N, permite ver los usuarios o dispositivos más activos y sus principales compañeros de conversación.

Filters

Permite a los paquetes ser comparados con una ecuación filtro. Los paquetes concordantes forman un stream que puede ser capturado o puede generar eventos. Sus elementos son: tipo de filtro bit (máscara y no máscara), filtro de expresión (nivel bit) y expresión condicional hacia otros filtros (and, or, not).

Packet capture

Permite que los paquetes sean capturados después de que fluyan a través del canal. Sus elementos son: tamaño del buffer para los paquetes capturados, buffer lleno (alarma) y número de paquetes capturados.

Events

Provee la habilidad para crear entradas en una bitácora de eventos y envía mensajes SNMP a la estación de administración. Los eventos pueden originarse de modificaciones a cualquier variable RMON. En adición a las cinco etiquetas estándar requeridas por SNMP (*link up, link down, warm start, cold start* y *authenticación failure*), RMON adiciona dos más: *rising threshold* y *falling threshold*.

El uso efectivo de los grupos RMON ahorra tiempo; en lugar de tener que observar gráficas en tiempo real para ocurrencias importantes, se puede depender del grupo Events para la notificación. A través de las etiquetas SNMP, los eventos pueden ejecutar otras acciones, proporcionando un manera automática de responder a ciertas ocurrencias.

4.5.1.2. Beneficios

Usar RMON conlleva tres ventajas principales:

- *Eficiencia*
  Usar el RMON remoto permite situarse en una estación de administración y recolectar información de segmentos LAN o VLAN ampliamente dispersos. Esto significa que el tiempo necesario para llegar al problema, configurar el equipo y comenzar a recolectar información es reducido significativamente.

- *Administración proactiva*
  Si está configurado correctamente, los RMON remotos entregan información antes de que los problemas ocurran. Esto significa que se pueden tomar acciones antes que se afecte a los usuarios. Además, los agentes remotos graban el comportamiento de la red, así que se pueden analizar las causas de los problemas.

- *Reducir carga en la red y en la estación de administración*
  La administración de red tradicional involucra una estación de administración verificando cada dispositivo de red a intervalos regulares para elaborar estadísticas e identificar problemas o cambios. Conforme crece el tamaño de la red y los niveles de tráfico, este método sitúa una gran carga de trabajo en la estación y también genera grandes cantidades de tráfico.
  Un RMON remoto, por otro lado, observa de manera autónoma la red evitando la intervención de la estación de administración y sin afectar las características y el rendimiento de la red. El extremo remoto

reporta sobre excepción, lo que significa que solo informa a la estación de administración cuando la red a entrado a un estado anormal.

4.5.2. SNMP

La figura 41 muestra un típico sistema de administración de red. Consiste de una estación de trabajo, conectada vía un router y el núcleo de la red a las redes de alto desempeño a administrar.

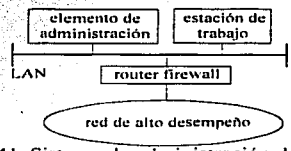


Figura 41. Sistema de administración de red

El elemento de administración generalmente va a ser una plataforma Unix corriendo el software SNMP. Por si mismo, es un protocolo directo de pregunta/respuesta que permite el intercambio de información de agentes localizados en cada componente de la red [bib04]. El agente obtiene la información de una MIB (*Management Information Base*) localizada dentro de cada componente. Los comandos "*Get*" pueden ser usados para obtener los parámetros MIB, descubriendo los componentes de red, y los comandos "*Put*" pueden establecer parámetros MIB, lo que permite configuración de los componentes. SNMP también permite a los componentes de red enviar alarmas y son parte del sistema de administración.

La tarea del sistema de administración SNMP es proveer un control con vistas gráficas de la red, resaltando nodos con problemas. El usuario va a ser capaz de usar la interfaz gráfica para situarse en dichos nodos y llevar a cabo un diagnóstico más detallado (usualmente a través de TCP/IP Telnet para acceder al router). El sistema de administración es también capaz de elaborar estadísticas y preparar reportes para asistir en las revisiones a largo plazo y la planeación de la capacidad de la red.

El elemento de administración es conectado a la red de alto desempeño vía una LAN o router. El router va a llevar a cabo una función de seguridad firewall, para proteger al sistema. Múltiples usuarios pueden ser acomodados añadiendo estaciones extras, las cuales pueden tener sesiones con la estación de administración.

Existen dos métodos para conocer el estado de los nodos:

- *Alarma o proceso de captura*. Los componentes de red tienden a producir una gran variedad de mensajes notificando eventos. Estos mensajes son enviados usando el protocolo SNMP, y atrapados por el sistema de administración. El sistema requerirá de un filtro de alarmas para que solo los eventos más serios sean notificados al operador. En lo posible, algunos tipos de alarmas deben ser desactivados para evitar tráfico innecesario.

- *MIB*. Obviamente, si un componente de red o su vía de comunicación hacia el sistema ha fallado, no se verán alarmas. Este problema es solucionado por el sistema verificando periódicamente los componentes de red. Esto puede ser hecho usando un *ping* (proceso mediante el cual un paquete de prueba es reflejado por el nodo en cuestión).

Alternativamente se puede usar SNMP para obtener una o más variables de las MIB. Estas son el depósito de información de los dispositivos de red y contiene una descripción de los objetos SNMP en la red y el tipo de información que proveen. Estos objetos pueden ser hardware, software, o asociaciones lógicas como conexiones o circuitos virtuales. Los atributos de un objeto pueden incluir cosas como el número de paquetes enviados, entradas en la tabla de ruteo y variables específicas de protocolos para el ruteo IP.

Las estadísticas de red también se obtienen de la verificación de los componentes. En este caso, es necesario ejecutar una serie de comandos "*get*" SNMP para obtener los datos relevantes. Una MIB típica puede contener muchos Kbytes de información útil. Es muy fácil consumir excesivo ancho de banda y espacio en disco recolectando mucha información. Elaborar estadísticas cada 15 minutos usualmente provee una resolución adecuada. La información mínima necesaria podría ser:

- *Utilización del procesador*. Para predecir el lugar y el momento en que se pueden requerir equipos más robustos.
- *Memoria libre*. Para identificar donde se puede necesitar memoria adicional.
- *Utilización de enlaces*. Para identificar los sitios que necesitan más capacidad, o donde se necesita investigar como reducir la carga a través de una optimización.
- *Razón de pérdida de paquetes*. Los equipos (ej. routers) generalmente lidian con protocolos IP no orientados a conexión, y evitan la congestión de puertos simplemente descartando cualquier sobrecarga.
- *Razón de paquetes erróneos*. Los enlaces de acceso generalmente van a correr protocolos basados en tramas HDLC. Estas tramas incluyen un secuencia para el chequeo de trama, la cual es usada para detectar y descartar paquetes erróneos.

Mientras que esto resulta adecuado para administrar redes pequeñas, no es suficiente para satisfacer una red a gran escala, debido a:

- *Escalabilidad*. Un estación de trabajo, corriendo un software de administración, solamente puede verificar pocos cientos de elementos en la red. Una red de alto desempeño a gran escala puede consistir de miles de elementos.

- *Componentes propietarios*. No todos los componentes de red usan protocolos de administración basados en estándares. Pueden tener plataformas propietarias de administración, que proveen información equivalente.

Un sistema típico de administración a gran escala es mostrado en la figura 42. Consiste de un número de elementos de administración, algunos basados en estándares y otros propietarios. El número exacto de elementos va a depender de:

- La capacidad del software de administración.
- El poder de la plataforma.
- La frecuencia de las verificaciones y el volumen de información a recabar.

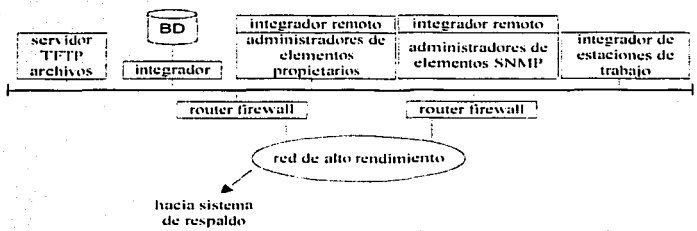


Figura 42. Sistema típico de administración a gran escala

Los elementos de administración se comunican con los dispositivos vía el backbone de la red y los routers firewall. Cabe mencionar, que en esta plataforma más compleja, las conexiones redundantes deben ser usadas para incrementar la disponibilidad de cada sitio.

El corazón de la plataforma es el software integrador. Este puede ser considerado como el administrador de administradores. Cada elemento de administración va a contener un integrador remoto diseñado para obtener información acerca de los elementos y después escribiendo la información en la base de datos. El servidor integrador genera las vistas de administración requeridas desde la base de datos hacia los clientes.
También es mostrado un servidor de archivos TFTP, el cual es usado para almacenar una imagen del software de los elementos de red y sus configuraciones.

Las técnicas empleadas en los ejemplos anteriores funcionan bajo ciertas reglas que están fundamentadas en toda la documentación referente al diseño de redes, pero es necesario cumplir con otras antes de iniciar algún proceso de cambio.

En el caso de la reubicación de equipo activo, es importante hacer notar que para realizar cualquier movimiento, debe conocerse a detalle la topología de red con la cual se está trabajando. Es común encontrar usuarios que por su conocimiento de las redes añaden equipo activo a su nodo de datos, incrementando el número de usuarios en ocho o doce, por lo regular. También habrá ocasiones en las que existan áreas que desde su nacimiento hayan sido colocadas en un lugar inadecuado de acuerdo a la topología, y con el paso del tiempo hayan crecido de tal manera que ya representan una carga de trabajo importante para la red. Peor aún, quizá no existan los medios físicos necesarios para reubicarlos dentro de un diseño adecuado. Es mas, tal vez exista un área con los recursos para llevar a cabo el mejor diseño posible, pero éste no sea compatible con el backbone de la UNAM.

Es en estos casos, cuando deben evaluarse las ventajas y desventajas de cada opción. A pesar de que la premisa para los casos presentados es la reubicación del equipo existente para lograr mejoras substanciales en el desempeño, no deberá olvidarse que existen límites respecto a lo que se puede lograr. Quizá llegará el momento en que no se pueda obtener mas del equipo instalado y sea necesario elaborar una propuesta que contemple la mejor solución posible, y alcanzable, sin embargo, se tendrá la seguridad de que el equipo actual cumplió con su tarea dentro del período de vida útil.

Conclusiones

A lo largo de esta exposición, se han tratado de analizar las diferentes opciones que se ofrecen para el diseño de la red que servirá de soporte a las actividades inherentes a la vida académica de la UNAM, haciendo mucho hincapié en la necesidad de planificar las diversas etapas hasta conseguir el establecimiento del mismo.

Aparte de los criterios comentados, en la planificación de la red han de tenerse en cuenta otros que protejan la inversión realizada.

Se ha de prever la evolución de la misma y adelantarse a los acontecimientos futuros: la red ha de ser lo suficientemente flexible para permitir la incorporación no traumática de nuevos elementos, ha de poseer una arquitectura abierta capaz de integrar diversos sistemas, y ha de permitir en todo momento el control sobre la misma. De esta forma, los usuarios tendrán acceso a los diferentes servicios y aplicaciones soportadas, obtendrán un alto grado de satisfacción por los mismos, y esto generará un mayor uso de ella y, por tanto, mejorará su rendimiento.

No debemos olvidar que el Internet está mejorando la calidad de la enseñanza, la investigación y la difusión. En el pasado, dicha calidad era determinada en gran medida por la ubicación geográfica y las actividades propias al entorno de desarrollo. Hoy, gracias al Internet, muchas de esas limitantes están desapareciendo permitiendo una expansión gradual hacia objetivos mas ambiciosos, lo que trae consigo la necesidad de mayores recursos y mejores herramientas.

También se ha visto un esfuerzo creciente por dotar de computadoras a la mayor cantidad de lugares posibles, desarrollar nuevas aplicaciones mucho mas especializadas, por un lado, o mas robustas, por otro, reducir los costos de los equipos activos e impulsar el Internet hacia nuevas fronteras.

Además, la tecnología está impactando mas allá de la calidad de la educación. También está preocupándose por la seguridad de la información, misma que se ha convertido en prioridad.

Los lugares que trabajan con un esquema de alta demanda han comenzado a tener una tendencia proactiva en la nueva administración de redes. Para lograr esto, es recomendable elaborar una teoría sobre el modelo OSI, la cual consta de nueve niveles, de los cuales, el ocho y el nueve son los que presentan más problemas, pues el octavo nivel somos nosotros mismos, los que estamos entre el teclado y la silla, los que normamos los procesos y estrategias de tecnologías de información (TI). De la misma manera, el noveno nivel imaginario es el mismo sitio, pues las redes deben empezar de ahí hacia abajo, no hacia arriba.

Del cuidado que se haya puesto en el diseño de la red dependerá en gran medida el resultado que se obtenga y, en consecuencia, el beneficio inherente que su utilización y explotación reportará, es por tanto necesario realizar estratégicamente la planificación de la red.

Glosario

10BASE-T. Especificación del IEEE para Ethernet 10Mbps sobre cable par trenzado categoría 3, 4 ó 5.

100BASE-FX. Especificación del IEEE para Fast Ethernet 100Mbps sobre cable de fibra óptica.

100BASE-TX. Especificación del IEEE para Fast Ethernet 100Mbps sobre cable par trenzado categoría 5 en adelante.

1000BASE-T. Especificación del IEEE para Gigabit Ethernet sobre cable par trenzado categoría 5 en adelante.

1000BASE-SX. Especificación del IEEE para Gigabit Ethernet sobre cable fibra óptica.

Adaptabilidad. La facilidad con la cual un diseño de red y su implementación pueden adaptarse a las fallas en la red, cambio en los patrones de tráfico, requerimientos adicionales u otros movimientos.

Administrable. La capacidad de una red de ser administrada y monitoreada, incluyendo la administración del rendimiento de la red, fallas, configuración, seguridad y accesos.

Agente. En administración de redes, proceso que reside en un dispositivo administrado y reporte valores de variables específicas a las estaciones de monitoreo.

Area. Segmentos físicos de una red y sus dispositivos conectados.

Autenticación. En seguridad, la verificación de la identidad de la persona o proceso.

Autorización. Asegurar una red especificando cuáles áreas (aplicaciones, dispositivos, etc) pueden ser accesadas por un usuario.

ATM. Asynchronous Transfer Mode. Estándar internacional para el envío de celdas en las cuales múltiples servicios (como voz, video o datos) son transportados en celdas de tamaño fijo (53-byte).

Backbone. La parte de una red usada como el camino principal para transportar tráfico entre los segmentos de red.

Balanceo de carga. La capacidad de distribuir el tráfico sobre todos los puertos que estén a la misma distancia de la dirección destino.

BPDU. Bridge Protocol Data Unit. Paquete utilizado en spanning tree enviado a intervalos establecidos para intercambiar información entre los bridge de una red.

Bridge. Dispositivo que interconecta dos LAN de diferente tipo para formar un sola red lógica que comprende los dos segmentos de red.

Broadcast. Paquete enviado a todos los dispositivos en la red.

Cliente. Nodo o programa que requiere servicios de un servidor.

Cliente/servidor. Sistemas de cómputo distribuido en los cuales las responsabilidades de transacción son divididas en dos partes: cliente y servidor. Los clientes dependen de los servidores para servicios tales como almacenamiento, impresión o capacidad de procesamiento.

Colisión. En Ethernet, el resultado de dos nodos transmitiendo simultáneamente.

Confiabilidad. Característica con la cual una red o sistema de cómputo provee un servicio libre de errores.

Congestión. Condición en la cual el tráfico ha alcanzado o se está aproximando a la capacidad total de la red.

Control de flujo. Técnica para asegurar que las entidades transmitiendo no saturen al receptor con información. Cuando la capacidad de recepción es alcanzada, un mensaje es enviado al dispositivo origen para que suspenda su transmisión hasta que la información almacenada sea procesada.

CSMA/CD. Carrier-sense Multiple Access with Collision Detection. Protocolo definido en los estándares Ethernet e IEEE 802.3 y en el cual los dispositivos transmiten solamente hasta encontrar un canal de datos libre dentro de un periodo de tiempo. Cuando dos dispositivos transmiten simultáneamente, ocurre una colisión y los dispositivos involucrados retrasan sus transmisiones durante un periodo de tiempo aleatorio.

Cuenta de saltos. Métrica de ruteo usada para medir la distancia entre un destino y un origen, en número de routers o saltos.

Dirección MAC. También conocida como dirección de hardware o física. Dirección de capa 2 asociada con un dispositivo de red en particular. La mayoría de los dispositivos que se conectan a una LAN tienen una dirección MAC asignada y que es utilizada para identificar otros dispositivos en la red. Las direcciones MAC tienen 6 bytes de longitud.

Diseño de red jerárquico. Técnica para diseñar topologías de red para campus o redes de alto desempeño empleando capas o módulos.

Disponibilidad. La cantidad de tiempo que una red está disponible a los usuarios, generalmente expresada como un porcentaje o mediante el MTBF y el MTTR.

Distance Vector. Algoritmo de ruteo que solicita a cada router el envío de su tabla mediante paquetes de actualización a sus vecinos periódicamente.

DNS. Sistema usado en Internet para la traducción de nombres de nodos de red a direcciones.

Dominio de colisión. En Ethernet, el área de red dentro de la cual las tramas que han colisionado son propagadas. Los repetidores y hubs propagan las colisiones; los switches LAN y routers no.

Encripción. Aplicación de un algoritmo específico para modificar la apariencia de la información, de manera que sea incomprensible para aquellos que no están autorizados.

Escalabilidad. Capacidad de una red de soportar cambios y crecimientos.

Ethernet. Especificación LAN desarrollada por Xerox, Intel y DEC. Las redes Ethernet usan CSMA/CD para transmitir paquetes a 10Mbps sobre una variedad de cables.

Fast Ethernet. Sistema Ethernet que está diseñado para operar a 100Mbps.

FastIP. Sistema para reducir la carga de los dispositivos de ruteo en las redes que tienen una gran cantidad de tráfico entre VLAN.

FDDI. Estándar LAN que especifica una red token-passing de 100Mbps usando fibra óptica con una arquitectura de doble anillo para proveer redundancia.

Filtering. El proceso de buscar en un paquete ciertas características, como dirección origen, dirección destino o protocolo. Filtering es usado para determinar que tráfico debe ser reenviado, y también puede evitar accesos no autorizados a la red o los dispositivos de red.

Firewall. Router o servidor de acceso remoto destinados a funcionar como un medio de contención entre redes, empleando listas de acceso que permitan la seguridad de la red.

FTP. File Transfer Protocol. Protocolo de aplicación, parte de TCP/IP, utilizado para la transferencia de archivos entre nodos de red.

Full duplex. Sistema que permite a los paquetes ser transmitidos y recibidos al mismo tiempo y, en efecto, duplicar el potencial de comunicación de un enlace.

Half duplex. Sistema que permite a los paquetes ser transmitidos y recibidos pero no al mismo tiempo. A diferencia de full duplex.

Handshake. Proceso mediante el cual dos entidades se sincronizan durante el establecimiento de la conexión.

Hub. 1. Término usado para describir un dispositivo que funciona como centro de una estrella. 2. En Ethernet, repetidor multipuerto, conocido como concentrador.

IANA. Internet Assigned Numbers Authority. Organización operada bajo el auspicio de ISOC que delega la autoridad para la asignación de direcciones IP, nombres de dominio y numeración de sistemas autónomos al NIC y otras organizaciones.

ICMP. Internet Control Message Protocol. Protocolo TCP/IP de la capa de red que reporta errores y provee información adicional relevante al procesamiento de paquetes IP. RFC 792.

IEEE. Institute of Electrical and Electronics Engineers. Organización fundada en 1963 que establece estándares para computadoras y comunicaciones.

IEEE 802.1D. Especificación que describe un algoritmo para prevenir loops al crear spanning tree.

IEEE 802.1P. Especificación que define GMRP y priorización de tráfico.

IEEE 802.1Q. Especificación que define el uso de VLAN.

IEEE 802.3. Protocolo LAN que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace. Utiliza el acceso tipo CSMA/CD a distintas velocidades y sobre diferentes tipos de medio.

IETF. Internet Engineering Task Force. Organización responsable de proveer soluciones para redes TCP/IP. En el área de administración de red, el grupo es responsable del desarrollo del protocolo SNMP.

IGMP. Internet Group Management Protocol. Sistema multicast filtering basado en IP que permite a las estaciones finales registrar que desean recibir tráfico de ciertos grupos multicast.

IP. Internet Protocol. IP es un protocolo de red capa 3 que es el estándar para enviar información a través de una red. IP es parte del conjunto de protocolos TCP/IP que describe el reenvío de paquetes a dispositivos direccionados.

IPX. Internetwork Packet Exchange. IPX es un protocolo de red capa 3 y 4 diseñado para redes que usan Novell Netware.

ISDN. Integrated Services Digital Network. Protocolo de comunicación, ofrecido por las compañías telefónicas, que permite a redes telefónicas transportar datos, voz y otro tipo de tráfico.

ISO. International Organization for Standardization. Organización internacional responsable de una variedad de estándares, incluyendo aquellos relevantes a las redes. ISO desarrolló el modelo de referencia OSI.

ISO 9000. Estándares internacionales de calidad-administración definidos por ISO. Los estándares, que no son específicos a cada país, industria o producto, permiten a la compañía demostrar que cuenta con los procesos adecuados para mantener un efectivo sistema de calidad.

ISOC. Internet Society. Organización internacional no lucrativa, que coordina la evolución y uso de Internet.

Kerberos. Sistema de autenticación que provee seguridad para protocolos de aplicación como FTP y Telnet.

LAN. Local Area Network. Red de estaciones finales (como PC's, impresoras, servidores) y dispositivos de red (hub's y switches) que cubren un área geográfica relativamente pequeña (usualmente no más grande que un piso o edificio). Las LAN se caracterizan por sus altas velocidades de transmisión a distancias cortas.

Latencia. El retraso entre el tiempo en que un dispositivo recibe un paquete y el tiempo en que el paquete es reenviado hacia el puerto destino.

Loop. Evento que ocurre cuando dos dispositivos de red están conectados por más de una camino, causando que los paquetes recirculen repetidamente alrededor de la red y no lleguen a su destino.

LsLAN. Large scale Local Area Network. Red de estaciones finales y dispositivos de red que cubren un área relativamente pequeña, sin embargo, junto con otras LAN forman un grupo de redes pertenecientes a la misma organización. Un caso práctico puede ser el cámpus de una universidad. También cuentan con equipos administrables e inclusive pueden contener características similares a los equipos de ruteo.

Llave privada. Código digital usado para desencriptar/encriptar información y proveer firmas digitales. Esta llave debe mantenerse secreta por el usuario; tiene un llave pública correspondiente.

Llave pública. Código digital usado para encriptar/desencriptar información y verificar firmas digitales. Esta llave puede distribuirse libremente; tiene un llave pública correspondiente.

MAC. Media Access Control. Protocolo especificado por el IEEE para determinar cuales dispositivos tienen acceso a la red en un momento dado.

Medio. Los distintos ambientes físicos a través de los cuales la señal de transmisión pasa. Los medios más comunes son el par trenzado, coaxial y fibra óptica y el aire (microondas, láser e infrarrojo).

Métrica de ruteo. Método por el cual un algoritmo de ruteo establece que una ruta es mejor que otra. Esta información es almacenada en tablas de ruteo. Las métricas incluyen ancho de banda, costo, retraso, cuenta de saltos, carga, MTU y confiabilidad.

MIB. Management Information Base. Conjunto de información acerca de las características y parámetros de un dispositivo. Las MIB son usadas por SNMP para recabar información acerca de los dispositivos en la red.

MTBF. Mean Time Between Failure. Tiempo promedio durante el cual persiste una falla en un sistema o red.

MTTR. Mean Time to Repair. Cantidad de tiempo promedio necesaria para reparar un sistema o red cuando falla.

MTU. Maximun Transmission Unit. Tamaño máximo de trama, en bytes, que una interfase en particular o medio puede manejar.

Multicast. Paquete enviado a un grupo específico de estaciones finales en la red.

Multicast filtering. Sistema que permite a un dispositivo de red reenviar tráfico multicast a una estación final solamente si ésta registró que desea recibir dicho tráfico.

Multiplexar. Esquema que permite a múltiples señales ser transmitidas simultáneamente a través de un solo canal físico.

NAT. Network Address Translation. Mecanismo para reducir la necesidad de direcciones IP globalmente únicas. NAT permite a una organización con direccionamiento privado, conectarse a Internet realizando la traducción hacia direcciones homologadas.

Negación de servicio. Ataque de seguridad en donde el intruso deshabilita el servicio de red, haciéndolo no disponible para los usuarios legítimos.

NIC. Network Interface Card. Interface de red.

OSI. Open System Interconnection. Modelo que consiste de siete capas, cada una de las cuales especifica una función en particular como direccionamiento, control de flujo, control de errores, encapsulación, etc.

OSPF. Open Shortest Path First. Algoritmo de ruteo jerárquico de tipo link state, propuesto como sucesor de RIP. Las características incluyen ruteo con un costo asociado y balanceo de carga. RFC 2178.

Paquete. Unión lógica de información que incluye una cabecera conteniendo información de control y, generalmente, información de usuario.

Port trunk. Conexión que permite a los dispositivos comunicarse usando hasta cuatro enlaces en paralelo.

Redundancia. Duplicación de dispositivos, servicios o conexiones de tal forma que al momento de una falla, puedan absorber la carga de trabajo de los activos.

Repetidor. Dispositivo físico que regenera y propaga las señales eléctricas entre dos segmentos de red.

Retraso en propagación. Tiempo requerido por un paquete para viajar sobre la red, del origen al destino.

RIP. Routing Information Protocol. Protocolo de ruteo de tipo distance vector usado en los inicios de Internet. RFC 1058 y RFC 1723.

RMON. Remote Monitoring. IETF Remote Monitoring MIB. Una MIB que permite monitorear remotamente las LAN especificando hasta nueve grupos de información.

Router. Dispositivo que usa una o mas métricas para determinar el camino óptimo para que el tráfico sea enviado. Provee enlaces entre redes geográficamente separadas.

Ruta estática. Ruteo explícitamente configurado en la tabla de ruteo.

Sistema autónomo. Colección de redes o áreas bajo con una administración en común, compartiendo una misma estrategia de ruteo.

Servidor. Nodo o programa que provee servicio a los clientes.

SMTP. Simple Mail Transfer Protocol. Protocolo de Internet utilizado en el servicio de correo electrónico.

SNMP. Simple Network Management Protocol. Actual protocolo IETF para administrar dispositivos en una red TCP/IP.

STP. Spanning Tree Protocol. Sistema basado en bridges para proveer tolerancia a fallas en las redes. STP permite implementar caminos paralelos para el tráfico, y asegura que los enlaces redundantes sean deshabilitados cuando los principales estén operacionales y viceversa.

Subred. En redes IP, una red compartiendo una dirección en particular. Las subredes son arbitrariamente segmentadas con el fin de proveer estructuras de ruteo multinivel y jerárquicas.

Switch. Dispositivo que interconecta varias LAN para formar una sola LAN lógica que comprende varios segmentos de red. Los switches son similares a los bridges en el hecho de que ambos conectan LAN de diferente tipo, sin embargo, son más sofisticados.

TACACS. Terminal Access Controller Access Control System. Protocolo que provee autenticación de acceso remoto. Las contraseñas son administradas en una base de datos central en lugar de routers individuales.

TCP/IP. Transmission Control Protocol/Internet Protocol. Este es el nombre de dos de los más conocidos protocolos desarrollados para la interconexión de redes. TCP/IP es ahora soportado en casi todas las plataformas, y es el protocolo de Internet.

Telnet. Protocolo de aplicación TCP/IP que provee un servicio de terminal virtual, permitiendo a un usuario iniciar una sesión en otro sistema y tener acceso como su estuviera conectado directamente en el dispositivo.

Token passing. Método de acceso mediante el cual los dispositivos utilizan el medio físico de manera ordenada basados en la posesión de una pequeña trama llamada token.

Topología. Disposición lógica de una red dentro de una estructura.

Utilización. Porcentaje de la capacidad usada en una red, respecto al total disponible.

VLAN. Virtual LAN. Grupos de dispositivos independientes de localización y topología que se comunican como si estuvieran en la misma LAN física.

VLAN tagging. Sistema que permite que el tráfico de múltiples VALN se transportado en un solo enlace.

WAN. Wide Area Network. Red de comunicación que cubre una gran área. Una WAN puede cubrir una extensa área geográfica y puede contener muchas LAN's.

WWW. World Wide Web. Red conformada por servidores de Internet que proveen hipertexto y otros servicios a terminales ejecutando aplicaciones cliente como los navegadores.

Bibliografía

Leon-García / Widjaja
Communication networks
McGraw-Hill, 2000 [bib01]

Mark Norris / Steve Pretty
Designing the total area network
Wiley-BT, 2000 [bib02]

Patrick H. Corringan
LAN disaster, prevention and recovery
PTR Prentice Hall, 1994 [bib03]

Cisco Systems / Cisco Press, Priscilla Oppenheimer
Top down network design
Macmillan Technical Publishing, 1999 [bib04]

Cisco Systems, Diane Teare
Designing Cisco Networks
Cisco Press, 1999 [bib05]

Catálogo de productos
IBDN Certified catalog
NORDX/CDT, 2001 [bib06]

3com
Switch management guide
3com Technologies, 2000 [bib07]

3com
Switch user guide
3com Technologies, 2000 [bib08]

Revista
Universidad de México
Marzo-Mayo 2001 [bib09]

Sarai Peñaloza Jezabel
Sistema de nombres de dominio
Tesis 1999 [bib10]

Revista en línea acerca de la tecnología de la información
http://www.itworld.com [bib11]

Revista de información especializada en redes y telecomunicaciones
http://www.red.com.mx [bib12]

Información relacionada a DHCP
http://www.dhcp-handbook.com/dhcp_faq.html [bib13]

Compañías dedicadas al desarrollo de productos relacionados al Internet
http://www.3com.com [bib14]

Compañías dedicadas al desarrollo de productos relacionados al Internet
http://www.cisco.com [bib15]

Instituto Nacional de Estadística, Geografía e Informática
http://www.inegi.gob.mx [bib16]

Internet Society. Encargada de difundir información sobre el Internet
http://www.isoc.org [bib17]

Asociación Nacional de Universidades e Instituciones de Educación Superior
http://www.anuies.mx [bib18]