UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Análisis del desempeño de la red de datos de la DEPFI y propuestas para su actualización

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A N

Juan Manuel Jiménez Chávez
José Esteban López Ovando
Diego Iván Rocha Mendoza

DIRECTOR DE TESIS

Ing. Alejandro Velázquez Mena

Ciudad Universitaria, Cd. Mx., 2004

OBJETIVO

Optimizar el desempeño de la red de datos, con base en las necesidades de comunicación de datos de la DEPFI, sus capacidades tecnológicas y sus planes de desarrollo.

MOTIVACIÓN

La elaboración del servicio social la llevamos al cabo en el Departamento de Sistemas de la DEPFI, UNAM. Una de las problemáticas que percibimos fue el mal funcionamiento de la red de datos de dicha dependencia.

La red de datos de la DEPFI ha presentado problemas como bajo ancho de banda (velocidad de transmisión baja), pérdida de acceso a RED-UNAM e Internet, mal funcionamiento de equipos de red (e.g. Hubs, switch's, transceiver's, etc.), problemas de seguridad, tales como intrusiones y ataques cibernéticos, propagación de virus, etc.

Además, no existe el equipo humano responsable de la administración de la red, así como la información descriptiva de la red, tal como planos, mapas de distribución de equipos de red, topología utilizada, etc.

El propósito de esta propuesta de tesis es el dotar a la DEPFI de la información necesaria para administrar y dar mantenimiento a su red de datos, así como una solución al mal funcionamiento de la misma.

Actualmente se pretende que la DEPFI se integre a Internet 2 y que cuente con salas de videoconferencia. El resultado de la tesis propuesta podría coadyuvar a la realización de dichos proyectos.

La relevancia de esta propuesta radica en la actualización de la red de datos de la DEPFI, así como la obtención de la documentación necesaria para su administración.

INTRODUCCIÓN

Hoy en día, las tecnologías de la información y las telecomunicaciones constituyen una herramienta esencial para la producción, transmisión y difusión del conocimiento. Al mantenerse actualizada tecnológicamente, la UNAM conserva su liderazgo que desde 1958 ha tenido en este ámbito, tanto en el país como en América Latina.

La RedUNAM es una compleja Red de Redes, pionera y líder en México, que transporta simultáneamente enormes volúmenes de paquetes de voz, datos y video. Es una de las redes educativas de telecomunicaciones digitales de mayor densidad y más avanzadas en América Latina. Cumple con la tarea estratégica de intercomunicar a la Comunidad Universitaria entre sí, y a ésta con el resto de la comunidad académica y científica mundial.

La División de Estudios de Posgrado de la Facultad de Ingeniería de la UNAM, hoy Secretaría de Posgrado e Investigación, necesita de una infraestructura de telecomunicaciones que le permita estar a la vanguardia tecnológica, y así brindar servicios informáticos de calidad y alta disponibilidad a la Comunidad Universitaria.

Los beneficios que se podrán tener al contar con una infraestructura de telecomunicaciones actualizada son:

- Crear estrategias que ayuden a la Institución a trabajar en conjunto con otras instituciones educativas y el sector productivo para estimular, iniciar y desarrollar aplicaciones educativas y de desarrollo socioeconómico.

- Dotar a la Comunidad Universitaria de acceso a comunicaciones de banda ancha, así como de aplicaciones de Internet, que puedan satisfacer necesidades educativas y de investigación que contribuyan al mejoramiento de la calidad de la formación académica.

El presente trabajo de tesis tiene como propósito brindar un diagnóstico de la infraestructura actual de la Red de Datos de la DEPFI, y proponer soluciones para su uso óptimo.

Con el diagnóstico realizado, al igual que con las propuestas de solución presentadas en este documento, se pretenden brindar las bases necesarias que le permitan a la DEPFI fortalecer su infraestructura de red de datos. Todo esto en términos de herramientas de hardware y telecomunicaciones de vanguardia, así como de recursos humanos calificados que apoyen la administración de la infraestructura.

Como preámbulo, en el primer Capítulo se describen los conceptos generales de las redes de datos, que forman el marco conceptual en el que se basa el presente trabajo. Con esto, se pretende familiarizar al lector con los conceptos utilizados en capítulos posteriores.

En el segundo Capítulo se dan a conocer las características generales de los sistemas de Cableado Estructurado. Se mencionan los subsistemas que lo conforman, los estándares internacionales así como la Norma Mexicana. Una vez conocidas las características y conceptos de Cableado Estructurado se hace referencia a algunos factores que hay que considerar para implantar un sistema de cableado.

El tercer Capítulo contiene información acerca de la evolución de las telecomunicaciones y su participación e importancia en la UNAM. Además se realiza una descripción cronológica de la red de datos de la Facultad de Ingeniería.

Como primer acercamiento se presenta la información recopilada de la Red de Datos de la DEPFI. También se proporciona un breve resumen del documento que plasma los lineamientos a los cuales deberán apegarse todas aquellas dependencias dentro de la Facultad de Ingeniería. Como parte final, se da a conocer un sumario del estado actual de la Red de Datos de la DEPFI, cuya información se utilizará en los siguientes capítulos.

En el cuarto Capítulo se realiza un análisis del estado actual de la Red de Datos de la DEPFI, el cual consiste en describir de forma detallada la topología física y lógica en la que está estructurada la red. En este sentido, se proporciona una descripción de la distribución y el número de equipos activos con los que se cuenta.

Para poder realizar un análisis a detalle, se hace uso de varias herramientas de software, con las cuales se pueden determinar las medidas de desempeño que tiene la red y poder conformar los resultados de este análisis.

Como parte del análisis de la topología lógica, se hace mención del Request for Comments 1918 (RFC 1918) que marca los lineamientos a seguir en cuestiones del espacio de direcciones IP para redes privadas que pueden ser usadas.

Por último, se mencionan la situación en la que se encuentra el cableado estructurado de la red, así como la situación administrativa.

El quinto Capítulo se dedica a la descripción de las propuestas de solución a los problemas detectados. Se proponen una serie de acciones que logren mejorar el desempeño de la red de datos de la DEPFI, en base a sus necesidades de comunicación de datos, las tendencias de crecimiento en el uso de la red y las tecnológicas.

CAPÍTULO 1

CONCEPTOS GENERALES DE REDES

En este capitulo se introducen los conceptos generales de las redes de datos que forman el marco conceptual en el que se basa el presente trabajo.

Se familiarizará con los modelos de referencia que describen las funciones que una red genérica necesita proporcionar. El Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI) y la Suite TCP/IP son los modelos en los que se basa este trabajo.

Posteriormente, se hace mención de la serie de estándares 802 de la IEEE que establecen los lineamientos a seguir para el cableado físico y la transmisión de datos en redes de área local.

En las tres secciones subsecuentes se describen las características principales de las Redes de Área Loca y Área Amplia, así como los dispositivos que se emplean para la comunicación de datos.

Por último, se trata el tema de Internet en donde se da una breve historia hasta el surgimiento de la Internet 2 (I2), de la cual se mencionan sus características principales, su estado actual en nuestro país y algunas de las aplicaciones desarrolladas en I2.

1.1 Definición de Red

La tecnología de comunicaciones en red tiene que ver con aquellas teorías de la ingeniería eléctrica, la ingeniería en computación y la ciencia de la computación y su aplicación a todos los tipos de comunicaciones sobre redes. Una red se define como un conjunto de nodos interconectados y enlaces. Un enlace lleva información desde un nodo a otro que está directamente conectado a él. Un nodo se comporta como un nodo final, un nodo intermedio, o ambos. Si el nodo se comporta como un nodo final, la información se origina o termina ahí. Un nodo intermedio redirecciona la información de un enlace a otro.

Con la llegada de las computadoras, el término red de comunicación de datos entró en boga. Ésta también es llamada red de comunicaciones de computadoras. La infraestructura de telecomunicaciones fue y sigue siendo usada para la comunicación de datos.

Objetivos de las redes de Datos

- Compartir recursos, equipos, información y programas que se encuentren geográficamente dispersos o locales.
- Brindar confiabilidad en la información.

- Transmitir información entre usuarios distantes de manera rápida, segura y económica.
- Obtener una buena relación costo/beneficio.

1.2 EL Modelo de Referencia de Interconexión de Sistemas Abiertos

El objetivo básico de una red es comunicar y compartir aplicaciones o dispositivos entre diferentes nodos. Debido a la amplia variedad de tipos de redes disponibles y la necesidad frecuente de interconectarlas, el problema de la interconexión de redes es tan importante que la ISO creó el Modelo de Referencia de Interconexión de Sistemas Abiertos (Open Systems Interconnection, OSI), que describe las funciones que una red genérica necesita proporcionar. El Modelo de Referencia OSI se ha convertido en la base para muchos estándares de comunicaciones de datos. Dado que los estándares son de dominio público, son llamados estándares abiertos. La ventaja del uso de los estándares abiertos es que cualquier compañía puede construir hardware o software para su uso en la red. Si se han cumplido los estándares, cualquier componente de diferentes fabricantes puede interoperar correctamente.

El Modelo de Referencia OSI explícitamente identifica siete capas funcionales organizadas jerárquicamente para comunicaciones en red, las cuales son: aplicación, presentación, sesión, transporte, red, enlace de datos y física (Ver Figura 1.1)

En el modelo OSI cada capa de red en el nodo emisor realiza un conjunto particular de funciones para su correspondiente capa de red en el nodo receptor, y esa misma capa confía en la siguiente capa inferior para realizar funciones más primitivas y para ocultar los detalles de dichas funciones. Idealmente, las capas deberían estar definidas de tal forma que los cambios en una capa no requieran cambios en las demás capas. Esto es, la capa de aplicación en el nodo emisor prepara los datos para la capa de aplicación en el nodo receptor. La capa de aplicación entonces pasa el mensaje a la capa de presentación. La capa de presentación da formato adecuado al mensaje para la capa de presentación del nodo receptor y lo pasa a la capa de sesión, y así sucesivamente. Cada capa tiene una interfaz bien definida a través de la cual se comunica con las capas adyacentes.

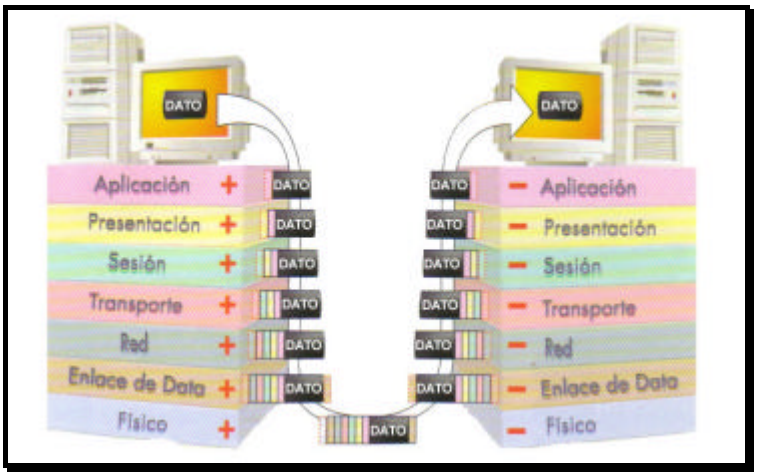


Figura 1.1 Modelo de Referencia OSI

Funciones básicas de las capas OSI

Capa 1: Capa Física. Esta capa es responsable de transmitir físicamente datos a través del medio de comunicaciones. Ésta especifica cómo se representan los datos en el medio, las características mecánicas y eléctricas de las conexiones físicas que deben existir entre el medio y la computadora, la velocidad a la cual la transmisión ocurre y el procedimiento para establecer, mantener y activar el enlace físico.

Capa 2: Capa de Enlace de Datos. Esta capa se encarga de preparar los mensajes para la transmisión física al siguiente nodo. Envía bloques de datos (frames) con la sincronización, control de errores y control de flujo necesarios. Algunas funciones específicas que lleva a cabo son: detección de errores a bajo nivel, delinear datos y establecer el protocolo a través del cual un nodo puede enviar y recibir datos.

Para LANs, la funcionalidad de la capa de enlace de datos es generalmente dividida en dos subcapas: control de enlace lógico (LLC, por sus siglas en inglés) y control de acceso al medio (MAC).

Capa 3: Capa de Red. Es responsable de colectar datos de contabilidad y rutear (routing) el mensaje. Es responsable de establecer, mantener y terminar conexiones a través de redes. Evita la necesidad de las capas superiores de conocer acerca de las tecnologías de transmisión y conmutación utilizadas para conectar sistemas. La tarea de contabilidad es responsable de llevar el número de mensajes recibidos así como su fuente y destino. La tarea de routing va de lo simple a lo complejo. En una LAN esta tarea es simple: el mensaje es transmitido a todos los nodos de la red. El transmitir un mensaje es práctico debido a que la alta velocidad de transmisión de la LAN y el área geográfica limitada aseguran una entrega veloz. En WANs y redes interconectadas, el routing es considerablemente más complejo. Puede existir una amplia variedad de rutas a través de las cuales el mensaje puede ser transmitido. Se utilizan diferentes tecnologías para encontrar la ruta de transmisión óptima. La capa de red escoge la o las rutas más apropiadas.

Capa 4: Capa de Transporte. La capa de transporte se asegura de que todos los mensajes sean entregados, que no haya mensajes perdidos o duplicados, y que los mensajes estén libres de errores, así como el control de flujo de los mensajes. La capa de transporte en el nodo receptor "le dice" a la capa de transporte del nodo emisor cuáles mensajes han sido recibidos exitosamente. Si un mensaje no es reconocido se vuelve a enviar. Además, la capa de transporte puede encargarse de optimizar el uso de servicios de red y de proporcionar una calidad de servicio requerida. Por ejemplo, la capa de transporte puede especificar tasas de error aceptables, retraso máximo, prioridad y características de seguridad.

Los mecanismos utilizados por el protocolo de transporte para proporcionar fiabilidad son muy similares a los utilizados por los protocolos de control de enlace de datos, como el HDLC, entre los cuales se encuentran el uso de números de secuencia, códigos detectores de errores y la retransmisión después de un tiempo determinado. La razón de este aparente duplicado de información

es que la capa de enlace de datos solo maneja un solo enlace directo, mientras que la capa de transporte maneja una cadena de nodos de red y enlaces. Aunque cada enlace en esa cadena es fiable debido al uso de HDLC, un nodo a lo largo de la cadena puede fallar en un momento crítico. Dicha falla afectará a los datos entregados, y es el protocolo de transporte el que maneja ese problema.

Capa 5: Capa de Sesión. Siempre que un objeto se comunica con otro, se dice que una sesión existe entre los dos. Las funciones generales de la capa de sesión son establecer una conexión entre dos aplicaciones, establecer las reglas de la conexión (comunicación simplex, half-duplex y full-duplex), controlar y terminar la misma. Algunas funciones específicas incluyen el control del flujo de datos entre objetos y recuperación si una falla ocurre.

Capa 6: Capa de Presentación. La capa de presentación acepta un mensaje de la capa de aplicación, aplica funciones para dar formato y luego pasa el mensaje a la capa de sesión. Los tipos de servicios de presentación que pueden ser realizados incluyen compresión de datos, cifrado de datos y conversión de fechas.

Capa 7: Capa de Aplicación. Las funciones específicas de esta capa son dependientes de la aplicación a ser ejecutada. En general, la capa de aplicación genera los datos para el mensaje a ser transmitido, le adjunta un identificador de transacción y posteriormente pasa el mensaje a la capa de presentación.

La Figura 1.2 muestra cómo la presencia de una red afecta la arquitectura OSI. Las tres capas más bajas tienen que ver con adjuntarse y comunicarse con la red. Los paquetes que son creados por el sistema final pasan a través de uno o más nodos de red que actúan como retransmisores entre los dos sistemas finales. Los nodos de red implementan las capas 1 a 3 de la arquitectura. En la figura, dos sistemas finales están conectados a través de un solo nodo de red. La capa 3 en el nodo realiza una tarea de conmutación y routing. En el nodo hay dos capas de enlace de datos y dos capas físicas. Cada capa, de enlace de datos y física, opera independientemente para proporcionar servicio a la capa de red sobre su respectivo enlace. Las cuatro capas superiores son protocolos fin-a-fin ("end-to-end") entre las máquinas comunicadas.

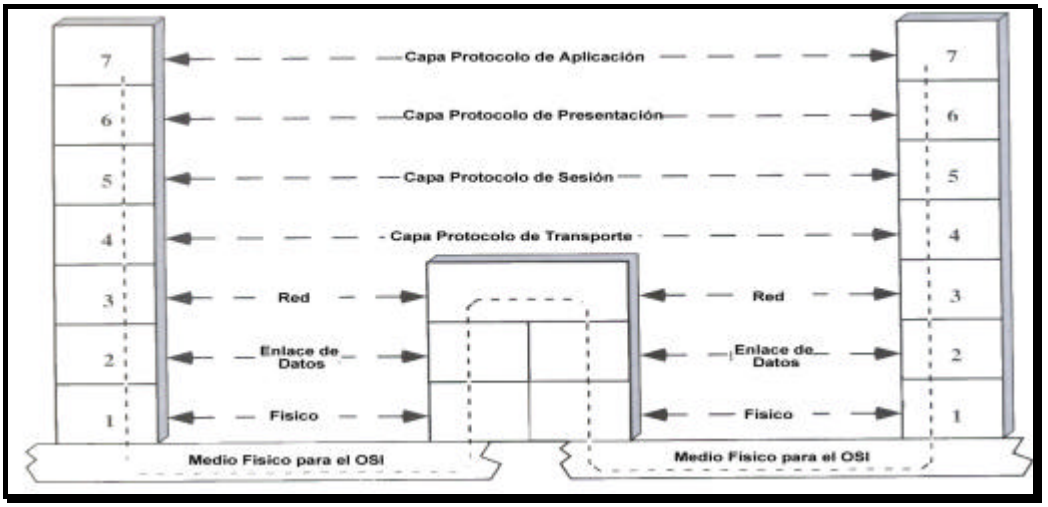


Figura 1.2 Interacción del medio físico y el modelo OSI

1.3 La Suite TCP/IP

Las siglas TCP/IP se refieren a dos protocolos de red, que son Transmission Control Protocol (Protocolo de Control de Transmisión) e Internet Protocol (Protocolo de Internet) respectivamente. Estos protocolos pertenecen a un conjunto mayor de protocolos. Dicho conjunto se denomina suite TCP/IP.

Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedamos a los distintos servicios de la Red. Estos servicios incluyen: transmisión de correo electrónico, transferencia de archivos, grupos de noticias, acceso a la World Wide Web, etc.

Hay dos clases de protocolos dentro de la suite TCP/IP que son: protocolos a nivel de red y protocolos a nivel de aplicación.

Protocolos a Nivel de Red

Estos protocolos se encargan de controlar los mecanismos de transferencia de datos. Normalmente son invisibles para el usuario y operan por debajo de la superficie del sistema. Dentro de estos protocolos tenemos:

TCP. Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de destino. En dicho punto, TCP se encargará de reensamblar dichos paquetes para reconstruir el archivo o mensaje que se envió. Por ejemplo, cuando se nos envía un archivo HTML desde un servidor Web, el protocolo de control de transmisión en ese servidor divide el archivo en uno o más paquetes, numera dichos paquetes y se los pasa al protocolo IP. Aunque cada paquete tenga la misma dirección IP de destino, puede seguir una ruta diferente a través de la red. Del otro lado TCP reconstruye los paquetes individuales y espera hasta que hayan llegado todos para presentárnoslos como un solo archivo.

IP. Se encarga de repartir los paquetes de información enviados entre la computadora local y las computadoras remotas. Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de las dos computadoras. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino por el camino más corto posible.

Protocolos a Nivel de Aplicación

Aquí tenemos los protocolos asociados a los distintos servicios de Internet, como FTP, Telnet, Gopher, HTTP, etc. Estos protocolos son visibles para el usuario en alguna medida. Por ejemplo, el protocolo FTP (File Transfer Protocol) es visible para el usuario. El usuario solicita una conexión a otra computadora para transferir un archivo, la conexión se establece, y comienza la transferencia.

Durante dicha transferencia, es visible parte del intercambio entre la máquina del usuario y la máquina remota (mensajes de error y de estado de la transferencia, como por ejemplo cuantos bytes del archivo se han transferido en un momento dado).

En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan intranets usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP.

Operación de TCP/IP

TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se ilustra en la figura siguiente:

EQUIPO SERVIDOR O CLIENTE	
Capa de Aplicaciones	Cuando un usuario inicia una transferencia de datos, esta capa pasa la solicitud a la Capa de Transporte.
Capa de Transporte	La Capa de Transporte añade una cabecera y pasa los datos a la Capa de Red.
Capa de Red	En la Capa de Red, se añaden las direcciones IP de origen y destino para el enrutamiento de datos.
Capa de Enlace de Datos	Ejecuta un control de errores sobre el flujo de datos entre los protocolos anteriores y la Capa Física.
Capa Física	Ingresa o egresa los datos a través del medio físico, que puede ser Ethernet vía coaxial, PPP vía módem, etc.

Después de que los datos han pasado a través del proceso antes descrito, viajan a su destino en otra máquina de la red. Allí, el proceso se ejecuta al revés (los datos entran por la capa física y recorren la pila hacia arriba). Cada capa de la pila puede enviar y recibir datos desde la capa adyacente. Cada capa está también asociada con múltiples protocolos que trabajan sobre los datos.

Números IP

La versión actual del protocolo IP (la versión 4 o IPv4) define de esta forma direcciones de 32 bits, lo que quiere decir que hay 232 (4.294.967.296) direcciones IPv4 disponibles. Esto parece un gran número, pero la apertura de nuevos mercados y el hecho de que un porcentaje significativo de la población mundial sea candidato a tener una dirección IP, hacen que el número finito de direcciones pueda agotarse eventualmente. Este problema se ve agravado por el hecho de que parte del espacio de direccionamiento está mal asignado y no puede usarse a su máximo potencial.

Por otra parte, el gran crecimiento de Internet en los últimos años ha creado también dificultades para encaminar el tráfico entre el número cada vez mayor de redes que la componen. Esto ha creado un crecimiento exponencial del tamaño de las tablas de enrutamiento, que se hacen cada vez más difíciles de sostener.

La solución a largo plazo de estos problemas pasa por desarrollar la próxima generación del protocolo IP (IPng o IPv6) que puede alterar algunos de nuestros conceptos fundamentales acerca de Internet.

Clasificación del Espacio de Direcciones

Cuando el protocolo IP se estandarizó en 1981, la especificación requería que a cada sistema conectado a Internet se le asignase una única dirección IP de 32 bits. A algunos sistemas, como los routers, que tienen interfaces a más de una red se les debía asignar una única dirección IP para cada interfaz de red. La primera parte de una dirección IP identifica la red a la que pertenece el host, mientras que la segunda identifica al propio host. Por ejemplo, en la dirección 135.146.91.26 tendríamos:

Prefijo de Red	*Número de Host*
135.146	91.26

Esto crea una jerarquía del direccionamiento a dos niveles. Recordemos que la dirección es realmente una cadena de 32 dígitos binarios, en la que en el ejemplo anterior hemos usado los 16 primeros para identificar la red y los 16 últimos para identificar el host.

Clases Primarias de Direcciones. Con la finalidad de proveer la flexibilidad necesaria para soportar redes de distinto tamaño, los diseñadores decidieron que el espacio de direcciones debería ser dividido en tres clases diferentes: Clase A, Clase B y Clase C. Cada clase fija el lugar que separa la dirección de red de la de host en la cadena de 32 bits.

Una de las características fundamentales de este sistema de clasificación es que cada dirección contiene una clave que identifica el punto de división entre el prefijo de red y el número de host. Por ejemplo, si los dos primeros bits de la dirección son 1-0 el punto estará entre los bits 15 y 16.

Redes Clase A (/8). Cada dirección IP en una red de clase A posee un prefijo de red de 8 bits (con el primer bit puesto a 0 y un número de red de 7 bits), seguido por un número de host de 24 bits.

Es posible definir un máximo de 126 (2^7-2) redes de este tipo y cada red /8 soporta un máximo de 16,777,214 (2^{24}-2) hosts. Obsérvese que se han restado dos números de red y dos números de host. Estos números no pueden ser asignados ni a ninguna red ni a ningún host y son usados para propósitos especiales.

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para las redes /8 o clase A:

1/8 hasta 126/8

Redes Clase B (/16). Tienen un prefijo de red de 16 bits (con los dos primeros puestos a 1-0 y un número de red de 14 bits), seguidos por un número de host de 16 bits. Esto da un máximo de 16,384 (2^{14}) redes de este tipo, pudiéndose definir en cada una de ellas hasta 65,534 (2^{16}-2) hosts.

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para las redes /16 o clase B:

128.0/16 hasta 191.255/16

Redes Clase C (/24). Cada dirección de red clase C tiene un prefijo de red de 24 bits (siendo los tres primeros 1-1-0 con un número de red de 21 bits), seguidos por un número de host de 8 bits. Se tienen así 2,097,152 (2^{21}) redes posibles con un máximo de 254 (2^{8}-2) host por red.

El rango de direcciones en notación decimal para las redes clase C sería:

192.0.0/24 hasta 223.255.255/24

Subredes

En 1985 se define el concepto de subred, o división de un número de red Clase A, B o C, en partes más pequeñas. Dicho concepto es introducido para subsanar algunos de los problemas que estaban empezando a producirse con la clasificación del direccionamiento de dos niveles jerárquicos.

- Las tablas de enrutamiento de Internet estaban empezando a crecer.
- Los administradores locales necesitaban solicitar otro número de red de Internet antes de que una nueva red se pudiese instalar en su empresa.

Ambos problemas fueron abordados añadiendo otro nivel de jerarquía, creándose una jerarquía a tres niveles en la estructura del direccionamiento IP. La idea consistió en dividir la parte dedicada al número de host en dos partes: el número de subred y el número de host en esa subred:

Jerarquía a dos Niveles

Prefijo de Red	*Número de Host*
135.146	91.26

Jerarquía a tres Niveles

Prefijo de Red	*Número de Subred*	*Número de Host*
135.146	91	26

Este sistema aborda el problema del crecimiento de las tablas de enrutamiento, asegurando que la división de una red en subredes nunca es visible fuera de la red privada de una organización. Los routers dentro de la organización privada necesitan diferenciar entre las subredes individuales, pero en lo que se refiere a los routers de Internet, todas las subredes de una organización están agrupadas en una sola entrada de la tabla de rutas. Esto permite al administrador local introducir la complejidad que desee en la red privada, sin afectar al tamaño de las tablas de rutas de Internet.

Por otra parte, sólo hará falta asignar a la organización un único número de red (de las clases A, B o C) o como mucho unos pocos. La propia organización se encargará entonces de asignar distintos números de subred para cada una de sus redes internas. Esto evita en la medida de lo posible el agotamiento de los números IP disponibles.

1.4 Estándares IEEE 802

Una organización internacional influyente que establece estándares de comunicación es el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers). El IEEE es una sociedad profesional de científicos, técnicos y miembros que ejercen la enseñanza en más de 140 países. El comité de redes locales de la sociedad informática del IEEE ha desarrollado muchos estándares de redes que se utilizan actualmente. Especial mención tienen los estándares "802" sobre cableado físico y la transmisión de datos en redes de área local. El desarrollo de los estándares comenzó en 1980 con la creación del comité IEEE 802 y el proyecto 802. Las especificaciones 802 han ido derivando en varias categorías consecutivas (802.1, 802.2, y así sucesivamente). Los más conocidos son los estándares 802.3 y 802.5 para redes, aunque todos los estándares son importantes para la interconexión. A continuación se muestra una descripción de los estándares:

- ✓ 802.1: una introducción a los estándares 802
- ✓ 802.2: estándares para el control lógico de enlace (LLC, Logical Link Control) y otros estándares sobre la conexión básica de redes
- ✓ 802.3: estándares para el acceso múltiple con detección de portadora y con detección de colisiones (CSMA/CD, Carrier Sense Multiple Access/ Collision Detection)
- ✓ 802.4: estándares para el acceso al bus mediante el paso de testigo (token bus)
- ✓ 802.5: estándares para el acceso al anillo mediante testigo (token ring) y para la comunicaciones entre redes LAN y MAN
- ✓ 802.6: estándares para redes LAN y MAN, incluyendo interconexión de alta velocidad y sin conexiones
- ✓ 802.7: estándares para tecnología de banda ancha
- ✓ 802.8: estándares para tecnología de fibra óptica
- ✓ 802.9: estándares para servicios de red integrados, tales como voz y datos
- ✓ 802.10: estándares para seguridad de redes LAN y MAN
- ✓ 802.11: estándares para la conexión inalámbrica
- ✓ 802.12: estándares para el método de acceso con prioridad

- ✓ 802.14: estándares para comunicaciones de banda ancha en los canales de televisión por cable

1.5 Dispositivos de Red.

En una red un número de dispositivos trabajan en varias capas del modelo de referencia OSI para formar una red completa. Éstos son conocidos como dispositivos de interconexión o dispositivos de red.

Repetidor

Es un dispositivo de la capa física que restaura datos y señales de colisión, transmite todo el tráfico entre segmentos, incluyendo información de colisión. Este dispositivo incrementa el diámetro de la red y permite acceder a usuarios adicionales mientras que actúa como un amplificador para reforzar la señal.

En su forma más básica, un repetidor debería ser capaz de ejecutar las siguientes funciones:

1. Regeneración de la señal: la regeneración de la amplitud para compensar la atenuación debida al cable.
2. Regeneración del preámbulo, debido a que los bits de preámbulo se pierden comúnmente.
3. Particionamiento: un repetidor debería ser capaz de auto-particionar un segmento defectuoso y reconectar al segmento una vez que se haya alcanzado una operación normal.
4. Aplicación de colisión: cuando una colisión ocurre en un segmento, ésta debe propagarse a todos los segmentos de la red.
5. Extensión del fragmento: en general, los fragmentos son el resultado de las colisiones. Si no se extendiera, el fragmento se perdería debido a la pérdida del preámbulo.

Sin embargo, un repetidor en la red introduce algunas anomalías, entre las que se encuentran:

1. Retardo: un repetidor introduce retraso en la red debido a la regeneración del preámbulo y de la señal.
2. Encogimiento del IPG (Inter Packet Gap).
3. Topología limitada.

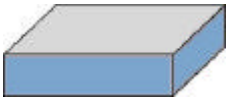


Figura 1.3 Simbología de un repetidor

Puente (Bridge)

Un puente es un dispositivo de la capa de enlace de datos que conecta dos o más dominios con colisiones. Multicast de MAC son propagados a través de "LAN extendida". Una LAN sobrecargada puede ser segmentada utilizando un puente. De acuerdo a la especificación IEEE 802.1, un puente MAC en una LAN 802.3 trabaja bajo el límite de servicio MAC, esto es, el servicio MAC y las capas LLC son transparentes a él.

Actualmente, los puentes son reemplazados mayormente por switch's (descritos más adelante). Un puente copia frames de una LAN a otra del mismo tipo o alguna extensión a una LAN de diferente tipo. Los puentes toman la decisión acerca de cuáles frames hay que copiar, con base en observaciones de las direcciones fuente en los frames recibidos. Esto los hace extremadamente útiles para la administración del tráfico en LANs. Pueden además ser configurados para filtrar frames basado en las direcciones. Un puerto de un puente (o interfaz de red) opera en modo promiscuo, aceptando todos los frames. Los frames son internamente almacenados, y la dirección destino es comparada con todas las direcciones en la base de datos de envío.

El proceso de examinar cada frame es conocido como filtrado. La tasa de filtrado está directamente relacionada con el nivel de desempeño del puente. En otras palabras, entre mayor sea la tasa de filtrado de un puente, será menor la probabilidad de que se convierta en cuello de botella. Otra cosa importante que hay que considerar de un puente es la tasa de envío. Ésta es usualmente expresada en frames por segundo y expresa la capacidad del puente de reenviar frames de un segmento de LAN a otro.

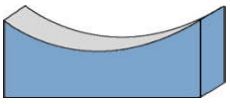


Figura 1.4 Simbología de un puente

Concentrador (Hub)

Este dispositivo trabaja en la capa dos del modelo OSI. La función principal del Hub es la de replicar la señal que ingresa por cada uno de sus puertos hacia el resto de los puertos, realizando así la difusión que requiere Ethernet (que se daba naturalmente en las topologías de bus sobre cables coaxiales).

Los Hubs también monitorean el estado de los enlaces de las conexiones a sus puertos, para verificar que la red funcione correctamente.

Figura 1.5 Simbología de un hub

Switch de capa 2

Tradicionalmente, para resolver una LAN sobrecargada, los puentes eran utilizados para segmentar la red. Desde entonces, la mayor demanda por el ancho de banda, administración de red, análisis de tráfico, y transmisión más rápida han llevado a los ingenieros a desarrollar un dispositivo más rápido con menor costo por puerto.

Estos switch's reciben la trama, y generalmente la transmiten por el puerto que corresponde. Cuando una estación envía una trama, el switch "aprende" la ubicación de dicha estación, y las tramas dirigidas a ella serán enviadas sólo por ese puerto, lo que mejora mucho el desempeño de la red.

Actualmente, los switch's representan una expansión en los conceptos del uso de puentes en Ethernet. Un número de atributos diferencian a los switch's de los puentes, entre los que se encuentran:

1. Los switch's están diseñados para proporcionar alta velocidad.
2. Cada puerto representa un segmento, proporcionando un número de segmentos LAN dentro de un límite de conmutación.
3. Pueden dar soporte a la segunda, tercera y cuarta capa (nivel experimental) del modelo OSI.
4. Capacidad avanzada de filtrado y administración.
5. Capacidad multi-entronque (MLT)
6. Opciones de apilamiento, etc.

Los switch's más recientes ofrecen uplinks FDDI, Fast Ethernet, Gigabit Ethernet, ATM o links con CAM para direcciones MAC.

Switch de Capa 3

Un problema de los routers tradicionales es que la mayoría de las decisiones de conmutación son hechas por un microprocesador muy costoso.

Para superar este costo, los switch's de Capa 3 utilizan ASICs baratos para realizar su conmutación. Esto reduce el costo de los switch's de capa 3, haciéndolos más baratos, por puerto, que un router tradicional.
De otra manera, los switch's de Capa 3 pueden hacer la mayoría de las tareas que un router realiza:

- Enrutan tráfico de Capa 3, como paquetes IP, basados en la dirección de destino.
- Pueden filtrar basándose en políticas configurada
- Pueden verificar el checksum de los paquetes de Capa 3.
- Actualizan la información SNMP MIB para propósitos de administración
- Actualizan la información de los paquetes de Capa 3, tal como el campo Time-To-Live (TTL) en IP.
- Soportan QoS

La mayoría de los switch's de Capa 3 están restringidos a uno o dos protocolos, y usualmente soportan un número restringido de tipos de medio. Por lo tanto, no son un reemplazo completo para el router tradicional. Sin embargo, debido a que están diseñados para manejar tráfico LAN de alto desempeño, un switch de Capa 3 puede ser situado en cualquier lugar dentro de un core de red o un backbone, reemplazando fácilmente y a un costo efectivo el router del backbone.

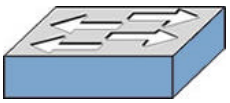


Figura 1.6 Simbología de un switch

Ruteador (Router)

Los ruteadores trabajan en la capa tres del modelo OSI, y de manera similar a los switch's y puentes, en el sentido de que filtran tráfico de la red por protocolos específicos en lugar de hacerlo por dirección de paquetes. Estos dispositivos fueron desarrollados debido a la necesidad de la división lógica de una red en lugar de una división física. Por ejemplo, un ruteador puede dividir una red en varias subredes de manera que el tráfico destinado a una dirección particular puede pasar entre segmentos. Dicho filtrado toma más tiempo que el usado por un puente o un switch que sólo observan la dirección MAC. Cuando se implementan ruteadores en redes más complejas, se mejora la eficiencia de la red.

El router puede unir diferentes tecnologías, siempre y cuando usen el mismo protocolo.

Figura 1.7 Simbología de un router

Pasarela (Gateway)

Este dispositivo trabaja en las siete capas del modelo OSI. El enfoque tradicional de los puentes y los ruteadores es resolver problemas inter-redes, en un ambiente donde todos los dispositivos implementan protocolos compatibles en las correspondientes capas del modelo OSI. Por ejemplo, protocolos de capa 3 (IP, IPX, etc.) para ruteadores y capa 2 (MAC) para puentes. Por su parte, los gateways realizan la conversión de protocolos a través de las siete capas del modelo OSI. En otras palabras, un gateway modifica los bits en el interior del paquete y esta función en particular puede ser combinada también en la enésima capa.

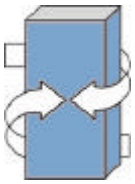


Figura 1.8 Simbología de un gateway

1.6 Redes de Área Local (LAN)

Una LAN es una red de datos de alta velocidad. Aunque, si bien es cierto, se pueden tener distintas definiciones de este concepto. Una primera idea de LAN sería tener dos o más computadoras conectadas, que se comunican entre sí a través de algún medio (cable coaxial, par trenzado, fibra óptica, microondas, etc.).

La IEEE define una LAN como: Sistema de comunicación de datos que permite un cierto número de dispositivos comunicarse directamente entre sí, dentro de un área geográfica reducida y empleando canales físicos de comunicación de alta velocidad.

Estas computadoras conectadas entre sí, comparten dispositivos periféricos y datos a una velocidad de transferencia de al menos 1Mbps. Normalmente, se localizan dentro de una zona limitada, como puede ser una oficina, o un piso de un edificio.

Algunas de las ventajas del uso de LAN son: el acceso compartido a dispositivos y aplicaciones y el intercambio de archivos entre los usuarios conectados. La distancia de operación en una LAN es menor de 10km.

Topologías de redes LAN

La disposición física de la red se denomina "topología". La arquitectura también determina la topología de la red de área local. Existen tres topologías básicas que son: estrella, bus y anillo. También podemos encontrarnos variaciones de las anteriores como las topologías en árbol, doble anillo y malla.

A continuación se describirán las características de cada una de las principales topologías que se pueden emplear en una LAN.

Topología Anillo

Una red con topología de anillo se organiza conectando los nodos en un ciclo cerrado. La ventaja de esta red es que se puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.

En una red de anillo, los nodos envían un paquete de datos conocido como token o contraseña de paso. El token contiene la dirección del emisor y la dirección del nodo receptor. Cuando el nodo receptor ha copiado el mensaje, regresa el token al nodo generador, el cual le envía luego el token al siguiente nodo del anillo. Si no tiene algo que enviar, el token pasa al nodo siguiente. Este método es conocido como Token Passing.

Cada nodo participa en dos enlaces, recibe datos de uno y los transmite al otro; su capacidad de almacenamiento, si tiene, es de sólo unos cuantos bits y la velocidad de recepción y de transmisión es igual en todos los nodos.

Los enlaces (líneas de comunicación) son simplex, por lo tanto la información fluye en un solo sentido en el anillo.

Algunas veces, estas redes utilizan esquemas de transmisión de señales para determinar qué nodo puede tener acceso al sistema de comunicaciones.

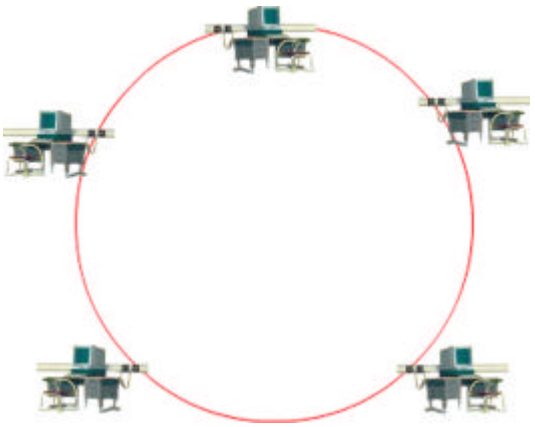


Figura 1.9 Topología de Anillo

Topología Bus

En la topología de bus todos los nodos están conectados a un bus compartido y tienen acceso igualitario a la red. Sin embargo, sólo un nodo puede tener el control en un tiempo dado. Un algoritmo determina qué nodo tiene el control de la LAN en un tiempo dado. Esta topología es utilizada en redes Ethernet y en configuraciones de redes de banda ancha. Debido a que las colisiones ocurren cuando más de una de estación tratan de tomar la LAN al mismo tiempo, el bus usualmente funciona por debajo de su eficiencia total.

Algunas de sus características son:

- Máximo 1024 nodos conectados en una sola red
- Distancia máxima entre nodos finales es menor que 2500m
- Trabaja a 10, 100 y hasta 1000 Mbps

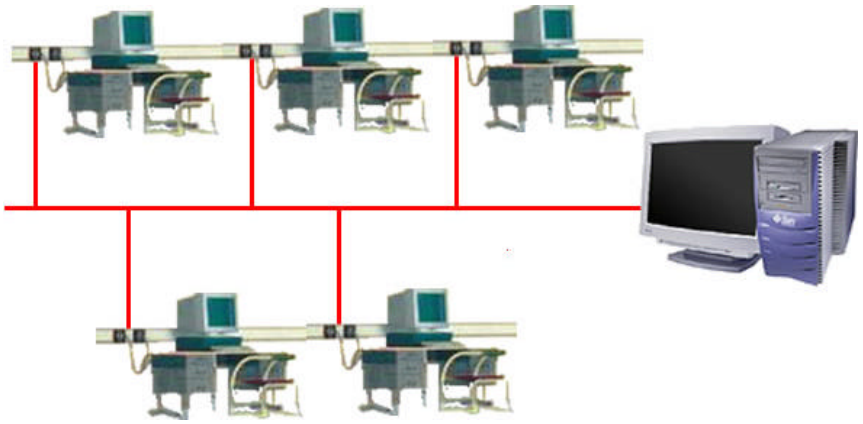


Figura 1.10 Topología de Bus

Topología Estrella

En la topología estrella el control de transmisión pasa a través de un dispositivo central de conexiones, conocido como concentrador de cableado, el cual controla el flujo de datos. Como se ilustra en la Figura 1.11, esta arquitectura facilita la adición de nuevas estaciones de trabajo a la LAN. Todo lo que se requiere es un cable que vaya del punto central de conexión a cada tarjeta de interfaz de red.

Otra ventaja de la topología de estrella es que el administrador de la red puede asignar a ciertos nodos un estatus mayor que a otros, dándoles prioridad de atención.

"Esta arquitectura hace posible contar con diagnósticos centralizados de todas las funciones de la red. Como todos los mensajes pasan a través del concentrador central es fácil analizar todos los mensajes emitidos por las estaciones de trabajo, y producir informes que revelen los archivos que utiliza cada nodo"[1].

La principal desventaja de una arquitectura de estrella es que si algo le sucede al dispositivo central, falla la LAN completa.

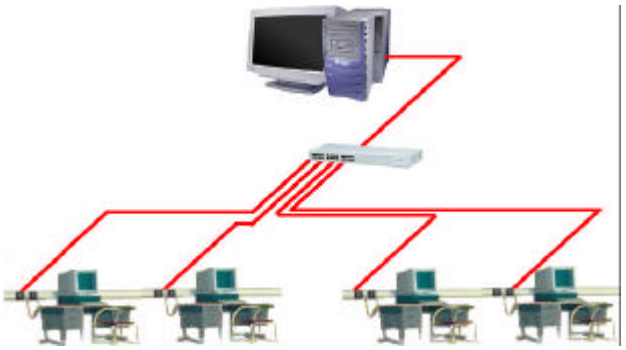


Figura 1.11 Topología de Estrella

[1] Jenkins, Neil & Schatt, Stan; Redes de Área Local (LAN); 5° ed; Prentice Hall; México, 1996.

Tecnologías de redes LAN

Ethernet

Existen varias tecnologías LAN, siendo Ethernet, Fast Ethernet y Gigabit Ethernet las más comunes. Una red puede estar basada en una o más de estas tecnologías. Las redes Ethernet, Fast Ethernet y Gigabit Ethernet funcionan de un modo similar, y la diferencia principal entre las mismas es la velocidad a la que transfieren la información. Ethernet opera a 10 Mbps, Fast Ethernet opera a 100 Mbps y Gigabit Ethernet opera a 1000 Mbps.

Ethernet fue originalmente desarrollado en 1973 en los laboratorios de la Corporación Xerox, en Palo Alto, California. En 1980, Xerox, DEC e Intel publicaron conjuntamente una especificación LAN basada en el concepto Ethernet. Una versión posterior fue ofrecida al comité 802.3 de la IEEE para su estandarización como una técnica de acceso LAN y fue aprobado para aquellas LAN que utilicen la técnica Carrier Sense Multiple Access with Collision Detection (CSMA/CD) en 1983. Desde entonces varias especificaciones IEEE 802.3 han sido escritas soportando varias tasas de transferencia y tipos de medio.

La norma IEEE 802.3 especificó la manera en que una LAN, que utilice la topología de bus, debe construir (y enviar a través de la red) los bloques de información para evitar colisiones; este protocolo es conocido como CSMA/CD. Igualmente, esta idea establece que cuando una estación desea transmitir, "escucha" la información que fluye a través del bus. Si el bus se encuentra ocupado, la estación espera hasta que esté en estado inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones, en forma simultánea, comienzan a transmitir en un bus inactivo, generan una colisión. Estas estaciones terminarán su transmisión, esperarán un tiempo aleatorio y repetirán todo el proceso.

Ethernet es la tecnología de red más popular actualmente. Muchos factores han contribuido a este éxito:

- Base instalada grande: más de 120 millones de computadoras personales, estaciones de trabajo y servidores interconectadas para 1996, de acuerdo con IDC.

- Facilidad de migración: debido a que el formato y el tamaño del frame son los mismos para todas las tecnologías Ethernet, ningún otro cambio en la red es necesario. Esto proporciona una ruta evolutiva de actualización. También, la disponibilidad de hubs cableados en estrella, tarjetas de interfaz de red (NIC, por sus siglas en inglés) con auto negociación y los switch's mejoran la ruta de migración.

- Escalabilidad: la estandarización de Fast Ethernet de 100 Mbps estableció a Ethernet como una tecnología escalable. Gigabit Ethernet extenderá esto aún más allá.

- Bajo costo: el precio por puerto para Fast Ethernet y Ethernet decrece rápidamente y la diferencia entre sus costos es cada vez más pequeña.

- Reentrenamiento mínimo: dado que el formato del frame y la topología de red de las diferentes versiones de Ethernet son las mismas, la capacitación del personal es mínima. También, todos los sistemas operativos populares y las aplicaciones son compatibles con Ethernet, así como los protocolos de capas superiores tales como TCP/IP, IPX, NetBEUI y DECNET.

- Alta confiabilidad en la red: la disponibilidad de herramientas de administración de la red y solución de fallas han contribuido a la alta confiabilidad de la red Ethernet.

Asimismo, en julio de 1993, un grupo de compañías de redes se reunieron para formar la alianza de Fast Ethernet. Este grupo incorporó un bosquejo de la especificación 802.3u 100BaseT de la IEEE, y aceleró la aceptación de dicha especificación en el mercado. La especificación final del 802.3u fue aprobada en junio de 1995.

Fast Ethernet, también llamado 100BASEX, es una extensión del estándar Ethernet IEEE 802.3, que opera a velocidades de 100 Mbps, un incremento diez veces mayor que el Ethernet estándar de 10Mbps. Otra aplicación de la tecnología Fast Ethernet es la tecnología 100BASE-VG de Hewlett-Packard, que opera a 100Mbps sobre un cableado UTP existente.

El proyecto Gigabit Ethernet comenzó en 1996 y fue terminado en junio de 1999. La intención era proporcionar 1Gbps de ancho de banda para backbone de redes y aplicaciones de estaciones de trabajo, además de ofrecer una ruta de actualización natural de las instalaciones actuales de 100 Mbps Fast Ethernet, al explotar las herramientas de administración de red y la capacitación.

Gigabit Ethernet emplea los métodos de control de flujo estándar de Ethernet para evitar congestión y sobrecarga.

Para acelerar la velocidad de Fast Ethernet de 100 Mbps a 1Gbps, se necesitaron grandes cambios en la Interfaz Física. Se decidió que Gigabit Ethernet pareciera idéntico a Ethernet en el nivel de enlace de datos.

El reto de superar la aceleración a 1 Gbps fue resuelto "mezclando" dos tecnologías: IEEE 802.3 Ethernet y ANSI X3 T11 Fiber Channel.

Con estas dos tecnologías juntas, el estándar puede aprovechar la alta velocidad de la tecnología de Fiber Channel, manteniendo el formato de frame de IEEE 802.3 de Ethernet, la compatibilidad con los medios instalados, y el uso de full o half duplex (vía CSMA/CD).

En la Tabla 1.1 se muestra el estándar IEEE 802.3, con todas las variantes de la tecnología Ethernet.

La Figura 1.12 muestra cómo el estándar IEEE 802.3 corresponde a las capas bajas del modelo OSI.

Estándar 802.3	*Tasa de Transferencia [Mbps]*	*Tipo de Medio*
1BASE-5	1	2 pares, 100 O Categoría 3 Par Trenzado (TP), máximo 250m
1BASE-5 (Thick Ethernet)	10	50 O coaxial, máximo 500m
1BASE-2 (Thin Ethernet)	10	50 O coaxial, máximo 185m
10BROAD36	10	75 O coaxial, máximo 1800m
10BASE-T	10	2 pares, 100 O Categoría 3 Par Trenzado (TP), máximo 100m
10BASE-F	10	62.5 µm, 160MHz Km, fibra óptica multimodo, máximo 2000m
100BASE-T4 (Familia Fast Ethernet)	100	4 pares, 100 O Categoría 3 Par Trenzado (TP), máximo 100m
100BASE-T2 (Familia Fast Ethernet)	100	2 pares, 100 O Categoría 3 Par Trenzado (TP), máximo 100m
100BASE-TX (Familia Fast Ethernet)	100	2 pares, 100 O Categoría 5 Par Trenzado (TP), máximo 100m
100BASE-F (Familia Fast Ethernet)	100	62.5 µm, 160MHz Km, fibra óptica multimodo, máximo 2000m, Full Duplex máximo 412m
1000BASE-CX (Familia Gigabit Ethernet)	1000	2 pares, 150 O Cuerda protegida de cobre*
1000BASE-SX (Familia Gigabit Ethernet) (longitud de onda corta)	1000	Fibra Óptica multimodo
1000BASE-LX (Familia Gigabit Ethernet) (longitud de onda larga)	1000	Fibra Óptica multimodo y modo simple
1000BASE-T (Familia Gigabit Ethernet)	1000	4 pares, 100 O Categoría 5 Par Trenzado (TP) más requerimientos del Boletín de Sistema Técnico (TSB) 95

* Este es un cable especial de fábrica

Tabla 1.1 Estándares IEEE 802.3

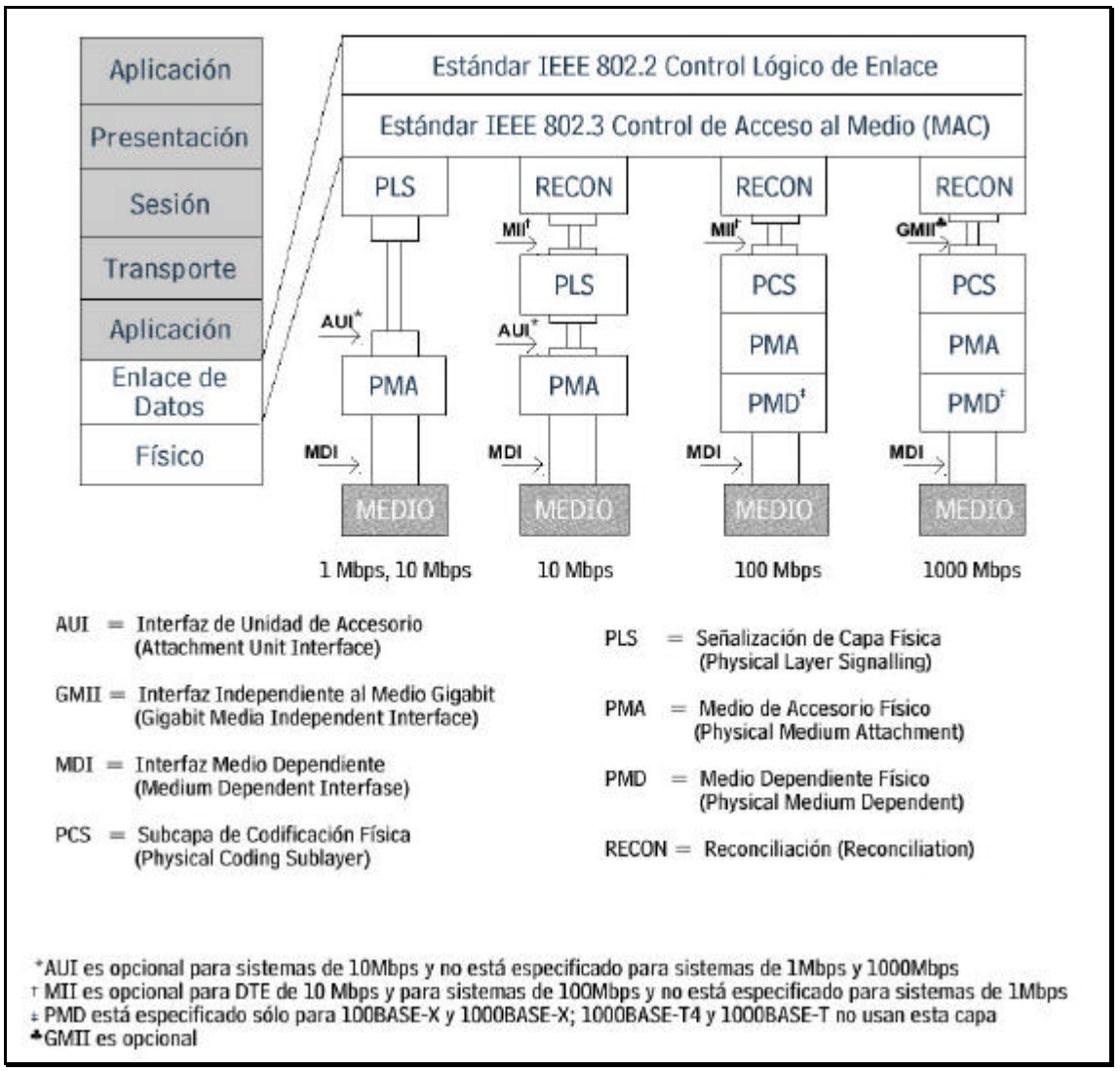


Figura 1.12 Correspondencia IEEE 802.3 - OSI

Además de las tecnologías LAN antes mencionadas, existen otras que están cayendo en desuso, entre las cuales podemos encontrar a Token Ring y Token Bus.

Token Bus

El estándar 802.4 del IEEE define un bus de señales. Aunque los nodos de un bus de señales codificadas pueden conectarse físicamente a un bus, ellos forman un anillo lógico. A cada nodo se le asignan posiciones lógicas en secuencia ordenada, con el último miembro de la serie seguido del primero. Cada estación debe conocer la identidad de los nodos que están antes y después de él. La configuración física del bus es irrelevante e independiente del ordenamiento lógico. La "señal codificada" en un sistema con bus de señales es un frame o paquete de control que regula el derecho al medio. Entre otras cosas, el paquete de la señal contiene una dirección destino. La estación destino, cuando se ha recibido la señal, recibe el control del medio por un tiempo determinado.

En el tiempo que una estación tiene el control sobre el medio, esta puede transmitir uno o más paquetes y puede examinar estaciones y recibir respuestas. Cuando expira el tiempo, o cuando el nodo ha terminado sus transmisiones, pasa la señal a la siguiente estación lógica. Por lo tanto, las transmisiones consisten en alternar secuencia de transferencia de señales codificadas y datos. Así mismo, un bus de señales puede permitir el paso a estaciones que no utilicen señales y que puedan responder solo a peticiones de reconocimiento.

Token Ring

Esta tecnología está definida en el estándar IEEE 802.5, que define un anillo de señales. Aunque el bus de señales codificadas debe pasarse por último por un anillo lógico, el anillo de señales es un anillo físico. La información se transfiere secuencialmente, bit por bit, de un nodo activo al siguiente. Cada nodo o estación sirve como medio para conectar uno o más dispositivos (como terminales y estaciones de trabajo) al anillo. Cada estación regenera y repite cada bit. La estación que tiene acceso al medio transfiere información al anillo, permitiéndole de esta manera ser leída por estaciones subsiguientes, y a esas estaciones direccionadas a su vez, copiar la información a medida que esta pasa. El generador de la información retira finalmente los datos del anillo.

La señal es definida por una secuencia única de transmisión de señales que circula en el medio después de cada transferencia de información. Después de la detección, cualquier estación puede capturar la señal modificándola.

Redes Virtuales de Área Local (VLAN)

Existen muchas definiciones acerca de lo que es una LAN Virtual (VLAN). Una VLAN puede ser descrita como un grupo de puertos en un switch o una agrupación de puertos en diferentes switch's. También puede ser caracterizada como un grupo de usuarios relacionados en la red de datos o un grupo de usuarios en la misma locación geográfica (que es lo más común). En el término más simple, una VLAN es un dominio de broadcast. Uno de los problemas al utilizar puentes para la segmentación de una LAN es que ellos resuelven problemas de ancho de banda, pero no de broadcast. Los switch's, aun cuando actúan básicamente como un puente, tienen características adicionales que los hacen más robustos al resolver problemas de red.

Las VLAN permiten utilizar los mismos medios físicos para formar varias redes independientes, a nivel de la capa 2 del modelo OSI. Se encuentran estandarizadas bajo la norma IEEE 802.1q.

"Las VLAN proporcionan al administrador de red la capacidad de romper una red puenteada en múltiples dominios broadcast. La ventaja de esta aproximación es que se puede realizar utilizando switch's que cuestan menos que los tradicionales router. Cada dominio broadcast, sin embargo, es

considerado una subred separada; para trasladarse entre subredes, un componente de capa tres, como un router aún es requerido."[2]

Una VLAN puede estar basada en el identificador de puertos de un switch, en la dirección MAC de una estación final, o en información del directorio o aplicación. También puede ser implementadas en varias formas diferentes, dependiendo de la topología del medio (Ethernet, FDDI o ATM).

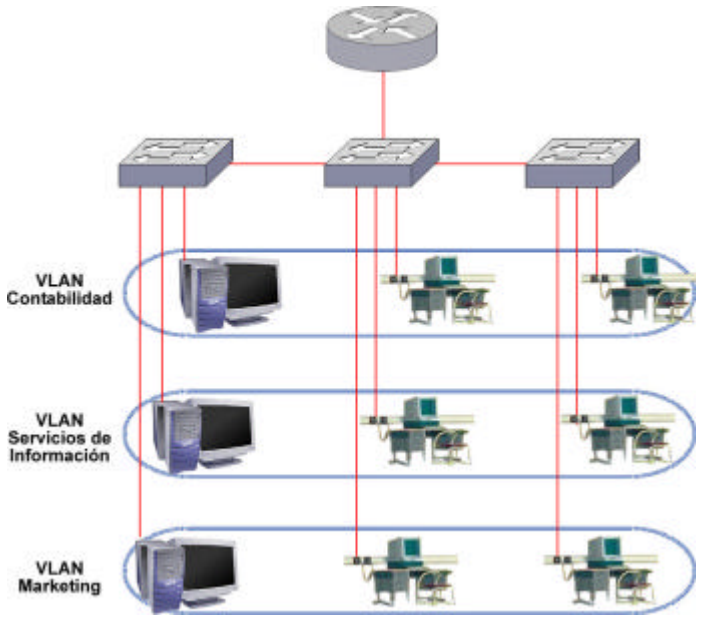


Figura 1.15 Representación física de una VLAN

1.7 Redes de Área Amplia (WAN)

Una WAN (Wide Area Network) constituye un sistema de comunicación que interconecta sistemas de computadoras (dos o más redes LAN) geográficamente remotos. Enlaza las computadoras situadas fuera de las propiedades de una organización (edificios o campus) y atraviesa áreas públicas que están reguladas por autoridades locales, nacionales e internacionales. Generalmente, el enlace entre lugares remotos se realiza a través de la red telefónica pública, pero una organización podría crear sus propios enlaces WAN mediante satélites, microondas u otras tecnologías de comunicación.

Las WAN generalmente utilizan protocolos punto a punto, de velocidades bajas a medias (usualmente menores a 2 Mbps), y se basan en servicios públicos o en líneas punto a punto.

Topologías de redes WAN

Las redes WAN están conectadas en topología de malla o de árbol.

[2] Deal, Richard A.; CCNP Swithcing Exam Cram; Coriolis, EEUU 2000.

Topología de malla

La topología de malla, como se muestra en la Figura 1.13, proporciona múltiples rutas entre nodos. Esto permite a los paquetes de un mensaje atravesar diversas rutas, y así balancear la carga de la red. También proporciona redundancia para la confiabilidad del servicio. Sin embargo, un mensaje broadcast de un nodo a todos los demás se volverá a transmitir en el modo broadcast por los nodos vecinos. Esto podría causar saturación en la red y la recirculación de paquetes, lo que necesita manejarse cuidadosamente. La saturación ocurre cuando un nodo retransmite el mismo paquete a todos los demás nodos y la recirculación ocurre cuando un paquete pasa alrededor de todos los nodos en un circuito. Una topología de malla es usualmente implementada con switch's y routers.

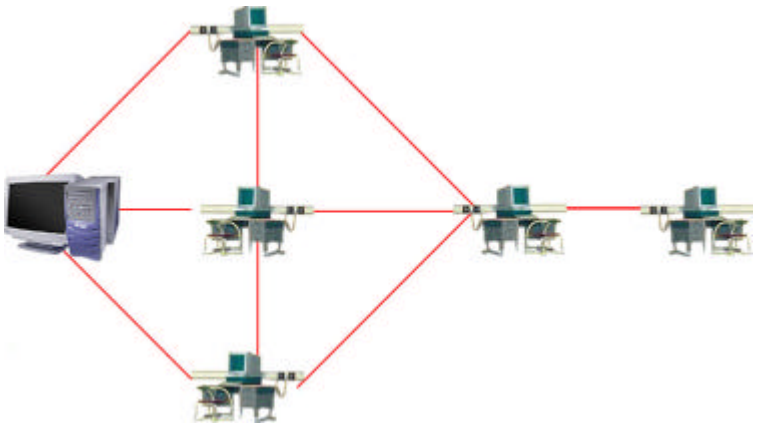


Figura 1.13 Topología de Malla

Topología de árbol

La topología de árbol es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (headend). Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

Esta topología es más simple de implementar que la topología de malla, usualmente utiliza bridges en la capa de enlace de datos del modelo OSI.

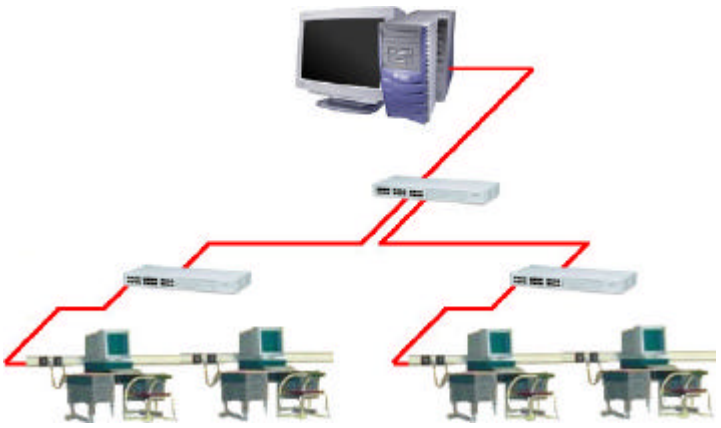


Figura 1.14 Topología de árbol

Tecnologías de redes WAN

WAN punto a punto

Una red de punto a punto es, sin duda, la más sencilla, ya que tiene sólo una computadora, una línea de comunicación y una terminal en el otro extremo del cable. Esta fue la primera forma de red existente, y muchas redes siguen conservando esta estructura, desarrollándose gradualmente en entidades más complejas. En un sistema de este tipo la computadora central no necesita ser muy grande. Una microcomputadora puede actuar como anfitriona de una o más terminales. Sin embargo, normalmente estos sistemas poseen una gran computadora como sistema anfitrión.

X.25

La recomendación X.25 define la interfaz entre un dispositivo terminal y una red de paquetes, incluyendo las capas física, de enlace de datos y de red, las cuales corresponden a las tres primeras capas del modelo OSI.

La capa física está definida en las recomendaciones X.21 y X.21 Bis. La capa de enlace X.25 consiste de frames que son transportados a través del uso del protocolo HDLC. La capa de red del X.25 consiste en paquetes que son transportados dentro del campo de información de los frames transportados por el protocolo HDLC.

La fácil accesibilidad a nodos de red de paquetes y el protocolo estandarizado X.25 hacen de esta red apropiada para conectar redes de área local dispersas, así como para obtener acceso a mainframes remotos.

"X.25 es el método preferido para el transporte de datos a baja velocidad y transmisiones con retraso intensivo que requieren la capacidad de corrección de errores proporcionada por la red X.25. Dado que la mayoría de las trasmisiones interactivas, tales como computadoras personales utilizadas como terminales, para acceder a una aplicación mainframe, son insensibles al retraso pequeño de 100ms de

un red X.25, se espera que tales redes permanezcan viables como un método de transporte de datos en un futuro." [3]

Frame Relay

Es un protocolo de enlace de datos en la capa 2 del modelo OSI, el cual define cómo los frames de datos son ensamblados y ruteados rápidamente a través de una red de paquetes. Frame Relay es estandarizado por el Comité ANSI T1 S1 y representa la primera interfaz de modo de paquetes a redes ISDN. Este protocolo surgió como sucesor de X.25 para redes de datos alta velocidad.

"Frame Relay está diseñado para soportar aplicaciones que requieren una velocidad de transferencia de datos alta con retrasos mínimos en la red, tales como aplicaciones LAN, transferencias de archivos grandes, aplicaciones de imágenes, y la interconexión de redes WAN de alta velocidad"[4].

La topología utilizada es una red de malla.

Características:

- Transmisión de tramas de longitud variable (hasta 1600 bytes)
- Alta velocidad de ráfagas. (servicio no garantizado)
- Actúa como un circuito virtual permanente
- Los nodos no efectúan control de errores ni de flujo
- Los enlaces están compartidos con otros clientes
- Pueden establecerse enlaces multipunto
- Están orientadas a la comunicación entre usuarios y proveedores de comunicaciones
- Las conexiones pueden ser Permanentes (PVC) o Temporales (SVC)
- Elementos de la red: Routers y Switch's

ATM

El modo de transferencia asíncrona (ATM) es una tecnología basada en celdas que puede usarse para alcanzar velocidades de transmisión de 1.2 Gbps. Cinco conceptos importantes comprenden esta tecnología:

- Circuito virtual-Ruta virtual
- Tamaño de paquetes fijos o células
- Tamaño de paquetes pequeños
- Multiplexación estadística
- Servicios integrados

[3] Held, Gilbert; Internetworking LAN´s and WAN´s; John Wiley & Sons. England, 1993
[4] Idem.

"La implementación de estas características en una red hecha de switch's ATM conduce a una red de alta velocidad que transporta los tres servicios multimedia (voz, video y datos). La calidad deseada del servicio está proporcionada para flujos individuales (a diferencia de la Internet actual) al mismo tiempo"[5].

Una de las ventajas de ATM es que, ya que todas las celdas tienen el mismo tamaño (53 bytes), es posible predecir los retardos de la red, lo que permite emplear este tipo de transmisión para transportar información de tiempo real, como voz y video. Esta tecnología está basada en un sistema de conmutación, lo que significa que se puede ampliar. Es posible manejar tráfico aun mayor, añadiendo conmutadores adicionales.

Las velocidades de los enlaces ATM pueden ser: 25.6 Mbps, 34 Mbps, 51.83 Mbps, 155.52 Mbps, 622.08 Mbps.

FDDI

El estándar interfaz de datos distribuidos por fibra (FDDI, Fiber Distributed Data Interface) se desarrolló hacia la mitad de los años ochenta para realizar comunicaciones de datos a mayor velocidad que las que ofrecía Ethernet (10 Mbps en aquellos años) o token ring (4 o 16 Mbps). El estándar FDDI está definido por el comité de estándares ANSI X3T9.5, y proporcionan un método de acceso que permite alta capacidad de datos en redes saturadas. Como la velocidad de los datos es de 100 Mbps, FDDI es una mejora sobre los 10 MBps de Ethernet. El medio de transmisión de FDDI es la fibra óptica. Un segmento FDDI de fibra óptica soporta hasta 500 nodos. La capacidad de comunicación es de 450.000 paquetes por segundo o hasta 10 veces la capacidad de las comunicaciones en Ethernet a 10 Mbps, que es de 15.000 paquetes por segundo como máximo. FDDI soporta tráfico de datos de voz, video y aplicaciones en tiempo real.

FDDI es parecido al método de acceso de token ring porque utiliza el paso de testigo en las comunicaciones de red. Difiere del estándar token ring en que utilizan un método de acceso de rotación cronometrada del testigo. Un testigo FDDI viaja por el anillo de la red desde un nodo hasta otro. Si un nodo no necesita transmitir datos, toma el testigo y lo envía al nodo siguiente. Si el nodo que posee el testigo necesita transmitir, puede enviar todas las tramas que desee durante un tiempo, llamado tiempo de retención del testigo. Es posible que varias tramas de varios nodos estén en la red en un tiempo determinado, proporcionando comunicaciones de gran capacidad, porque FDDI utiliza un método de liberación temprana de testigo.

Una vez que un nodo transmite una trama, ésta se desplaza hasta el próximo nodo del anillo. Cada uno de los nodos determinará si la trama está destinada a él y si existen errores en la trama. Si el nodo es el que tiene que recibir la trama, éste lo marca como leído. Si algún nodo detecta un error, marca un bit de estado para indicar una condición de error. Cuando la trama vuelve al nodo que originó la

[5] Subramanian, Mani; NETWORK MANAGEMENT; Addison-Wesley; EEUU, 2000

transmisión se lee de nuevo, para determinar si el nodo destino lo recibió. También se comprueban los errores de la trama, de manera que si se detectara un error se retransmitirá la trama. Si no se encuentran errores, el nodo que origino la transmisión sacara esa trama del anillo.

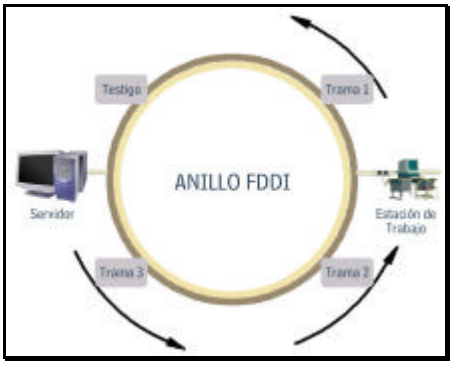


Figura 1.16 Método de acceso de rotación cronometrada del testigo

1.8 Internet e Internet 2

Internet

Internet fue creado a partir de un proyecto del Departamento de Defensa de los Estados Unidos llamado DARPANET (Defense Advanced Research Project Network) iniciado en 1969. El propósito principal de este proyecto era la investigación y desarrollo de protocolos de comunicación para redes de área amplia, para ligar redes de transmisión de paquetes de diferentes tipos.

Después de que las funciones militares de la red se separaron en una subred de Internet, la tarea de coordinar el desarrollo de la red recayó en varios grupos, uno de ellos la National Science Foundation de los Estados Unidos, quien promovió el uso de la red. Ésta se encargo de conectar cinco centros de supercómputo que podían ser accesados desde cualquier nodo de la red. Aunque funcionó bien al principio, pronto fueron superadas las cargas de tráfico previstas, y se dio la concesión a Merit Network Inc. para que administrara y actualizara la red. Se mejoraron las líneas de comunicación dando un servicio mucho más rápido.

El grupo de mayor autoridad sobre el desarrollo de la red es la Internet Society creado en 1990 y formado por miembros voluntarios, cuyo propósito fue promover el intercambio de información global a través de la tecnología de Internet. Tiene la responsabilidad de la administración técnica y dirección de Internet. El Internet Architecture Board (IAB), toma las decisiones acerca de los estándares de comunicaciones entre las diferentes plataformas para que puedan interactuar máquinas de diferentes fabricantes sin problemas. Es responsable de como se deben asignar las direcciones y otros recursos en la red, aunque no son ellos quienes se encargan de hacer estas asignaciones. Para ello existe otra organización llamada NIC (Network Information Center) administrado por el departamento de defensa de los Estados Unidos. Otro grupo importante es el Internet Engineering Task Force (IETF) en el cuál

los usuarios de Internet expresan sus opiniones sobre cómo se deben de implementar soluciones para problemas operacionales y cómo deben de cooperar las redes para lograrlo.

Internet 2

Después de 30 años de creada la ARPANET, los expertos advierten que apenas queda disponible un 40% de las direcciones y pronostican que en el 2005 estarán agotadas (según estudios de la IETF).

La proliferación de dispositivos conectados a Internet y las aplicaciones que los usuarios quieren utilizar (como tecnologías móviles, aplicaciones inalámbricas y comunicaciones en tiempo real) están llevando el IPv4 hasta su límite.

El proyecto Internet2 (I2) es un esfuerzo de colaboración para desarrollar tecnología y aplicaciones avanzadas en la Internet, vitales para las misiones de investigación y educación de las instituciones de educación superior.

Las más importantes universidades de todo el mundo, en colaboración con la industria y los gobiernos, encabezan este proyecto. Internet2 trabaja para hacer posibles aplicaciones tales como el aprendizaje remoto, la telemedicina, bibliotecas digitales y laboratorios virtuales que no son posibles con la tecnología del Internet de hoy.

Características

- Calidad de servicio (QoS)

La Calidad de Servicio es el efecto colectivo del desempeño de un servicio, el cual determina el grado de satisfacción a la aplicación de un usuario.

- Multicast

Es útil para enviar los mismos datos para diferentes usuarios. Mejora la utilización del ancho de banda. Disminuye el procesamiento nodo/enrutador y permite el envío de broadcast para quien lo quiera escuchar.

- MPLS (Multiprotocol Label Switching)

Es un método de routing de alto rendimiento para el envío de paquetes. Integra el rendimiento y el manejo de tráfico de la capa de enlace (Capa 2) con la escalabilidad y flexibilidad de la capa de red (Capa3). Integra routing IP con conmutación ATM ofreciendo escalabilidad en redes IP sobre ATM

- IPv6

El Internet Protocol versión 6 (IPv6) amplía las prestaciones del protocolo en uso actualmente: incrementa ampliamente el número de direcciones disponibles (utiliza 128 bits), habilita un routing más eficiente, permite una configuración más sencilla, incorpora una mejor seguridad en términos de autenticación e integridad del mensaje y privacidad, mejora el envío de datos en tiempo real,

proporciona una plataforma que permite mayor velocidad y cantidad de tráfico, entre otras características.

- H.323

El H.323 es una familia de estándares para videoconferencia definidos por el ITU. Está definido específicamente para tecnologías LAN que garantizan una calidad de servicio (QoS), Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

- Routing

Hace más eficiente el uso de los ruteadores, al utilizar una estructura jerárquica de las direcciones IP y tablas de routing más simples. Los protocolos que utiliza IPv6 son: RIPng o RIPv6, BGP4+, OSPFv6, EIGRPv6.

- Seguridad

Existen dos tipos de mecanismos de seguridad. El primero es la autenticación de los paquetes, realizada con el Authentication Header; el segundo es el cifrado "End-to-End" del paquete, realizada con el Encapsulating Security Payload Header.

Internet 2 en México

En México, el desarrollo de Internet ha entrado en las universidades. Se calcula que cerca de la mitad de los usuarios de Internet del país están ligados a las instituciones de educación superior

En la mayoría de los países avanzados del mundo, se han venido formando asociaciones para desarrollar redes educativas y de investigación de capacidad avanzada.

Existen universidades con proyectos de aplicaciones avanzadas de tecnologías de la información, que se utilizan para hacer más eficientes los procesos educativos y de investigación

Las principales universidades mexicanas han venido avanzando aceleradamente en el desarrollo de sus redes internas

- Fibra óptica en el campus
- Redes de Gigabit Ethernet y ATM de alta capacidad

Para buscar opciones de conectividad de mayor capacidad y mejor economía entre las instituciones de educación superior del país y de éstas con las del exterior, las universidades líderes del país decidieron integrar en México una red académica de la más avanzada tecnología.

Para manejar el proyecto de Internet 2 en México, el 8 de abril de 1999, se creo una asociación civil privada no lucrativa de instituciones académicas, denominada Corporación Universitaria para el Desarrollo de Internet, A.C. (CUDI).

El objetivo de CUDI es operar una infraestructura de telecomunicaciones entre las instituciones educativas y de investigación del país, basada en medios de transmisión de alta velocidad para:

- Apoyar la investigación y la educación
- Permitir el desarrollo de aplicaciones que impulsen la nueva generación de Internet

Conectividad

La Red utilizada para Internet 2 en México es patrocinada por las empresas Telmex y Avantel (Ver Figura 1.17). Se cuenta con un backbone de 8000km de enlaces a 155 Mbps. Además se cuenta con enlaces de 34Mbps hacia 16 universidades y sólo tienen acceso a la red las aplicaciones de Educación e Investigación.

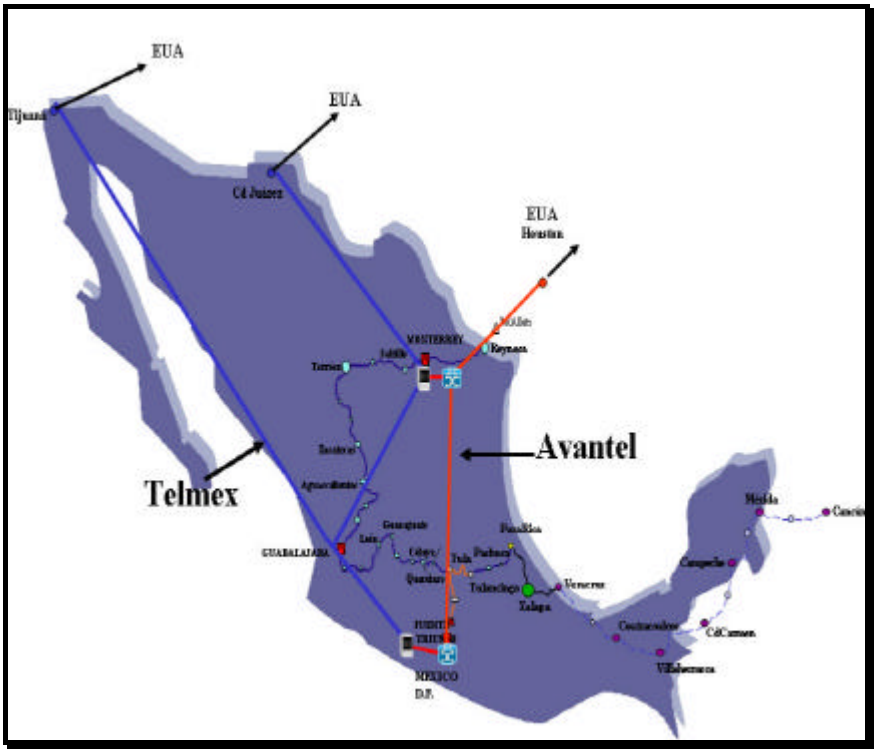


Figura 1.17 Backbone de I2 en México

Así mismo, la conexión internacional hacia los Estados Unidos se realiza en las ciudades de Ciudad Juárez, Monterrey y Tijuana, hacia ABILENE, VBNS Y CENIC, respectivamente, con enlaces de 100 Mbps en el primer enlace y 155 Mbps hacia los otros dos. (Ver Figura 1.18).

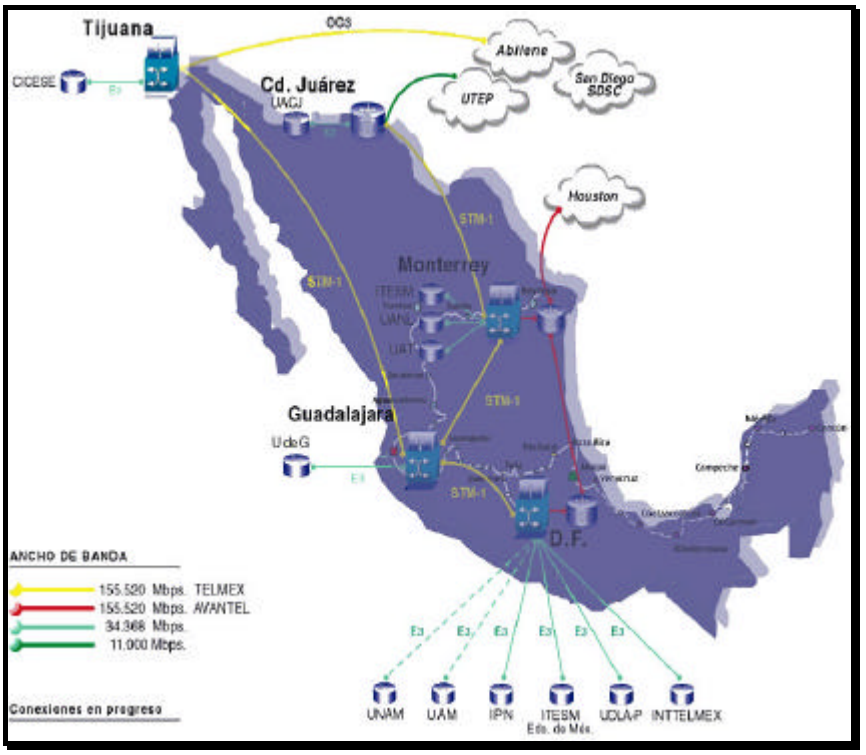


Figura 1.18 Conectividad de I2 en México

Aplicaciones de Internet 2

Las aplicaciones que utilizan Internet 2 son aquellas aplicaciones robustas que requieren de alta demanda de la red, transferencias masivas de datos, video en tiempo real, manipulación remota, calidad, seguridad, colaboración o alta disponibilidad de la red. Ejemplo de este tipo de aplicaciones son[6]:

- Educación a distancia. Cursos a distancia compartidos, por ejemplo, "Doctorado Conjunto en Telecomunicaciones entre UNAM y la Universidad Politécnica de Madrid"
- Bibliotecas digitales. Permite el acceso, entre otros, a publicaciones periódicas, por ejemplo "caso EBSCO".
- Telemedicina. Telesesiones Hospitalarias Interactivas, ejemplo de ello es el proyecto de "Telemedicina de la BUAP".
- Ciencias de la Tierra. Desarrollo del portal de Oceanografía por Satélite, del CICESE.
- Astronomía. Proyecto del Gran Telescopio Milimétrico del INAOE.
- Super Cómputo Compartido (Grid Computing). Grids-Supercómputo UNAM, Departamento de Supercómputo.
- Laboratorios Remotos. Sistema Interactivo de Investigación en Microscopía, de la UANL.
- Salud. Mapeo del Cerebro, BIRN (Biomedical Informatics Research Network), EEUU.
- Robótica. "Interacción Multilateral vía Internet con Robots Cooperativos", Mecatrónica, DEPFI, UNAM.

[6] www.cudi.edu.mx

CAPÍTULO 2

CABLEADO ESTRUCTURADO

Este capítulo describe los conceptos que están involucrados con los sistemas de cableado estructurado que, junto con los conceptos mencionados en el Capítulo 1, serán el sustento del análisis realizado en este trabajo.

En la primera sección se hace mención de los diferentes medios de transmisión que se usan en las redes de datos, así como las ventajas que ofrecen dichas tecnologías.

Se definen las características, ventajas y desventajas del Sistema de Cableado Estructurado. Posteriormente se mencionan los componentes físicos que se requieren para implementar un Sistema de Cableado Estructurado. Por otro lado, se describen los estándares fundamentales y la Norma Mexicana aplicables al Cableado Estructurado.

Finalmente se hace mención de algunas consideraciones importantes que se deben tomar en cuenta para diseñar un cableado estructurado.

2.1 Medios de Transmisión

Existen diferentes tipos de cables; la elección de uno respecto a otro depende del ancho de banda necesario, las distancias existentes y el costo del medio.

Cada tipo de cable tiene sus ventajas e inconvenientes; no existe un tipo ideal. Las principales diferencias entre los distintos tipos de cables radican en el ancho de banda permitido (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la amortiguación de la señal y la distancia recorrida.

En la actualidad existen básicamente tres tipos de cables factibles de ser utilizados para el cableado en el interior de edificios o entre edificios.

- Coaxial.
- Par trenzado.
- Fibra Óptica.

Cable Coaxial

Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

Originalmente fue el cable más utilizado en las redes locales (LAN) debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive.

Fig. 2.1 Componentes de un cable coaxial.

Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos.

Existen dos tipos de cable coaxial:

- Thick (grueso). Este cable se conoce normalmente como "cable amarillo", como se muestra en la Figura 2.2 y fue el cable coaxial utilizado en la mayoría de las redes. Su capacidad es mayor en términos de velocidad y distancia, pero el costo del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Este cable es empleado en las redes de área local conformando con la norma 10 Base 2.

Figura. 2.2 Cable Coaxial Thick (Grueso).

- Thin (delgado). Este cable se empezó a utilizar para reducir el costo de cableado de la red. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo, el cable es mucho más barato y delgado que el thick y, por lo tanto,

solventa algunas de las desventajas del cable grueso. Este cable es empleado en las redes de área local conformando con la norma 10 Base 5.

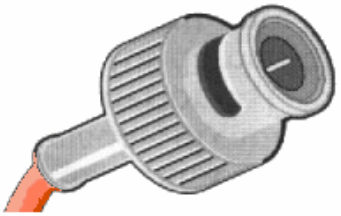


Figura 2.3 Cable Coaxial Thin (fino).

Cable Par Trenzado

Es el tipo más común y barato para la transmisión en la red. Este cable está compuesto de por lo menos dos alambres aislados, trenzados de manera que cada unión recibe la misma cantidad de interferencia del ambiente (ver Figura 2.4). Este ruido del ambiente se vuelve parte de la señal que se trasmite, el trenzado de los alambres reduce el ruido, aunque no lo elimina. Estos alambres vienen en un amplio rango de pares y calibres, los alambres tienen un calibre designado por AWG (American Wire Gauge), basado en su diámetro. Los cables de par trenzado más comunes para redes son los de calibre 22 y 24.

Hay dos tipos de cables de par trenzado. El cable de par trenzado sin blindaje (UTP) y el cable de par trenzado con blindaje (STP).

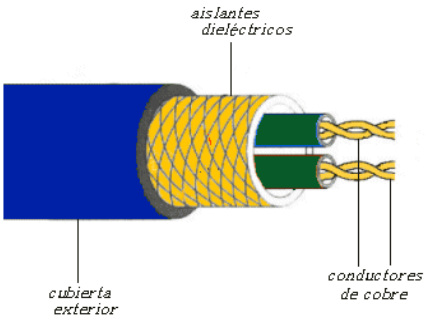


Figura 2.4 Cable de par trenzado (dos pares STP).

El cable de par trenzado está empaquetado en grupos de pares, el número de pares trenzados por grupo pueden variar en un rango de 2 a 3000. Entre más trenzado tenga el cable es menor la interferencia, y muchas de las LAN's implementadas utilizan 25 pares. Algunas utilizan el mismo cable de par trenzado sin blindar, que es el más económico y que se utiliza para los teléfonos, mientras que otras requieren un cable de mayor calidad para la transmisión de datos.

La principal desventaja de este tipo de cable es el rango limitado y la sensibilidad a las interferencias eléctricas. En un principio este tipo de medio podría manejar velocidades de transmisión de cerca de 1

Mbps a través de varios cientos de metros. En la actualidad la norma industrial 10BaseT muestra los avances tecnológicos que hacen posible transmitir información a 10 Mbps, mediante un cable de par trenzado y hoy en día se logra trasmitir a 1000 Mbps por medio de un cable de par trenzado sin blindar.

Cable de par Sin Blindaje (UTP)

El uso del cable UTP (Unshield Twiested Pair; Par Trenzado no Apantallado o sin blindar) se da en el sistema telefónico. Casi todos los teléfonos se conectan a las centrales telefónicas por un par trenzado.

Para tender varios kilómetros de par trenzado es necesario utilizar equipos que amplifiquen la señal, porque la misma pierde intensidad conforme se incrementa la distancia.

Las mayores ventajas de este tipo de cable son su bajo costo y su facilidad de manejo. Sus mayores desventajas son su mayor tasa de error respecto de otros tipos de cable, así como sus limitaciones para trabajar a distancias elevadas sin regeneración.

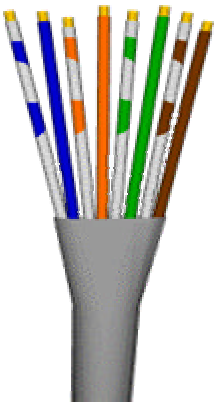


Figura 2.5 Cable UTP de cuatro pares

Para las distintas tecnologías de red local, el cable de pares de cobre sin blindar se ha convertido en el sistema de cableado más ampliamente utilizado.

El estándar EIA-568 en el Adendum TSB-36 diferencia tres categorías distintas para este tipo de cables.

Categorías

Existen opciones típicas de sistemas de Cableado Estructurado, cada una posee características de producto y de funcionamiento particulares.

CATEGORÍA	VELOCIDAD	APLICACIÓN
1	1Mbps	Datos de baja velocidad. Voz digital y análoga.
2	4Mbps	Datos de ISDN a 1.44 Mbps. T1: 1.544 Mbps. Voz digital. IBM3270,SYSTEM/3X,AS/400
3	16Mbps	10 base T. 4Mbps Token Ring. IBM 3270, 3X,AS/400. ISDN. Voz
4	20Mbps	10 base T. 16 Mbps Token Ring/Ethernet.
5	100Mbps	10 base T. 16 Mbps Token Ring/Ethernet 100 Mbps TDDI, FDDI
5e	100Mbps	Token Ring de 4 a 16 Mbps 10 Base T 100 Base TX AnylLan 100 Base VG ATM 155 y ATM 622 Ethernet Gigabit.
6	100, 155, 1000 Mbps	100 BASE TX ATM Gigabit Ethernet multimedia: audio digital AES/EBU control RS422 video analógico y digital NTSC/PAL y CATV Broadband,

Tabla 2.1 Categorías principales de aplicaciones del UTP

Algo que hay que notar en los pares de UTP es que siempre van polarizados. Dado que la compañía telefónica realiza su señalización y conmutación por medio de niveles de corriente directa, la polaridad debe ser mantenida en los conductores que se denominan tip y ring en inglés. Como en todos los sistemas de comunicaciones, se necesita un par dedicado de cables. Cada par consiste en un positivo (tip) y un negativo o de referencia (ring).

El porqué se usa UTP para cableado es de lo más sencillo de entender. Es el más empleado en el medio de las telecomunicaciones, ya que es muy barato y, cuando es correctamente instalado, es capaz de

un desempeño sobresaliente. El trenzado de cada par previene la interferencia que puede venir de otros pares del mismo cable y de fuentes externas, como pueden ser los motores o las líneas de potencia eléctrica.

Cable de par con blindaje (STP)

Cada par se cubre con una malla metálica, de la misma forma que los cables coaxiales, y el conjunto de pares se recubre con una lámina apantallante (Figura 2.6). Se referencia frecuentemente con sus siglas en inglés STP (Shield Twiested Pair, Par Trenzado Apantallado o con blindaje). El empleo de una malla apantallante reduce la tasa de error, pero incrementa el costo al requerirse un proceso de fabricación más costoso.

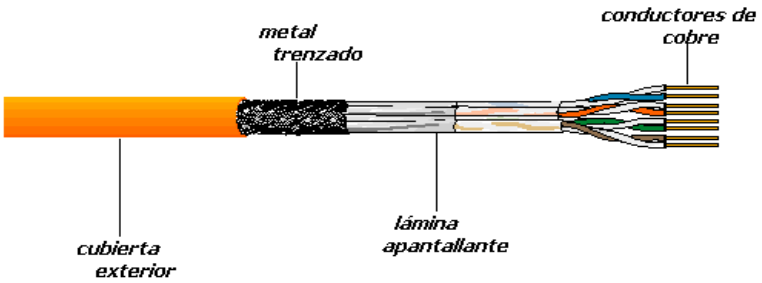


Figura 2.6 Cable SPT de cuatro pares.

Cable de fibra óptica

Este cable está constituido por uno o más hilos de fibra de vidrio. Cada fibra de vidrio consta de:

- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta de material similar que rodea al núcleo, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra.

La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta, y es convertida en señal eléctrica en el extremo receptor.

La fibra óptica es un medio excelente para la transmisión de información debido a sus características: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración. Su mayor desventaja es su costo de producción

superior al resto de los tipos de cable, debido a que se necesita el empleo de vidrio de alta calidad y la fragilidad de su manejo en producción.
La ventaja sobre los cables de para trenzado y coaxiales en la mayor velocidad de transmisión de datos.

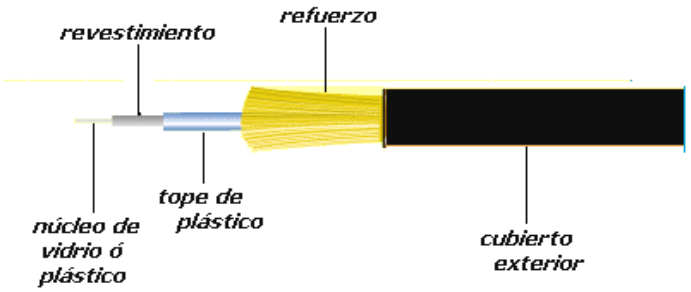


Figura 2.7 Partes de una fibra óptica.

La terminación de los cables de fibra óptica requiere un tratamiento especial que ocasiona un aumento de los costos de instalación.

Uno de los parámetros característicos de las fibras es su relación entre los índices de refracción del núcleo y de la cubierta, que depende también del radio del núcleo y que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional. Según el valor de este parámetro se pueden clasificar los cables de fibra óptica en dos clases:

Monomodo. Cuando el valor de la apertura numérica es inferior a 2.405, un solo modo electromagnético viaja a través de la línea y por tanto ésta se denomina monomodo.

Este tipo de fibras necesitan el empleo de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa (Figura 2.8). Resultan más caras de producir y el equipamiento es más sofisticado.

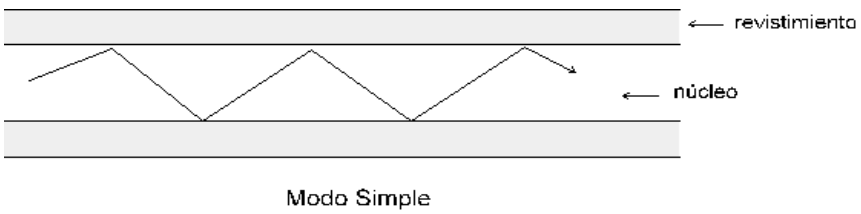


Figura 2.8 Fibra óptica monomodo simple

Multimodo. Cuando el valor de la apertura numérica es superior a 2.405, se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo (Figura 2.9).

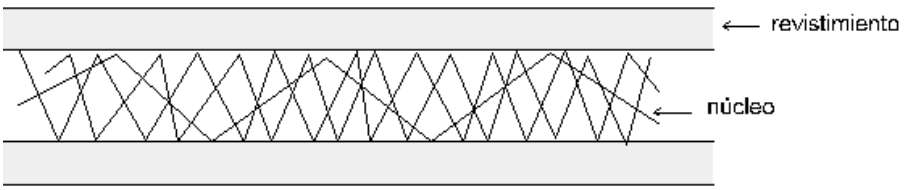


Figura 2.9 Fibra óptica multimodo

Las fibras multimodo son las más utilizadas en las redes locales por su bajo costo. Los diámetros más frecuentes 62.5/125 y 100/140 micras. Las distancias de transmisión de este tipo de fibras están alrededor de los 2.4km, y se utilizan a diferentes velocidades: 10 Mbps, 16 Mbps y 100 Mbps.

Las características generales de la fibra óptica son:

Ancho de banda: La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (sin blindaje/con blindaje) y el Coaxial. Aunque en la actualidad se están utilizando velocidades de 1.7 Gbps en la redes públicas, la utilización de frecuencias más altas (luz visible) permitirá alcanzar los 39 Gbps. El ancho de banda de la fibra óptica permite transmitir datos, voz, video, etc.

Distancia: La baja atenuación de la señal óptica permite realizar tendidos de fibra óptica sin necesidad de repetidores.

Integridad de datos: En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores o BER (Bit Error Rate) menor de 10^{-11}. Esta característica permite que los protocolos de comunicaciones de alto nivel, no necesiten implantar procedimientos de corrección de errores, por lo que se acelera la velocidad de transferencia.

Duración: La fibra óptica es resistente a la corrosión y a las altas temperaturas. Gracias a la protección de la envoltura es capaz de soportar esfuerzos elevados de tensión en la instalación.

Seguridad: Debido a que la fibra óptica no produce radiación electromagnética, es resistente al ruido. Para acceder a la señal que circula en la fibra es necesario partirla, con lo cual no hay transmisión durante este proceso, y puede por tanto detectarse.

Diafonía: Como una fibra óptica no radia, ni capta radiación externa, está completamente exenta de diafonía, lo que propicia una transmisión con muy buena calidad.

Existen varios tipos de conectores para fibra óptica, entre los cuales se encuentran los tipos SC, ST, MT-RJ, SMA, LC, MTP, FC, etc.

El adaptador ST (ver figura 2.10) para fibra óptica tiene al final dos conectores ST. El conector ST es usado como sistema de cerradura bayoneta. Simplemente hay que presionar y dar un cuarto de giro a éste, para fijar el conector. La limpieza de la fibra óptica es muy sencilla.

Figura 2.10 Conector para fibra óptica con terminales ST-ST

El adaptador SC (ver figura 2.11) para fibra óptica contiene al final dos conectores SC. El conector SC contiene una pequeña cerradura, que al presionar el conector se escucha un clic, para asegurarnos que la fibra está bien conectada.

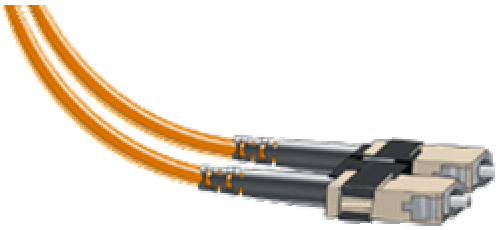


Figura 2.11 Conector para fibra óptica con terminales -SC - SC.

Las ventajas que tiene una fibra óptica son:

- Carencia de señales eléctricas en la fibra, por lo que no producen descargas eléctricas. Son convenientes por lo tanto para trabajar en ambientes explosivos.
- Liviandad y reducido tamaño del cable capaz de llevar un gran número de señales.
- Sin puesta a tierra de señales, como ocurre con los alambres de cobre que quedan en contacto con ambientes metálicos.
- Compatibilidad con la tecnología digital.
- Fácil de instalar.

Las desventajas que tiene la fibra óptica son:

- El alto costo.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibra roto en el campo.

2.2 Definición de Cableado Estructurado.

Un sistema de Cableado Estructurado es la infraestructura de cable destinada a transportar las señales desde un emisor hasta el correspondiente receptor. Está diseñado en una jerarquía lógica que adapta todo el cableado existente y el futuro, en un solo sistema.

El Cableado Estructurado es un plan completo de cableado para los edificios, que se basa en normas y estándares internacionales. Consiste en equipos, accesorios de cables y de conexión, así como de métodos de instalación y administración.

El sistema de Cableado Estructurado está diseñado para proporcionar una conexión física entre todas las zonas de trabajo de un edificio; se instala sin tener en consideración el tipo de equipo de comunicación al que se va a conectar, se adapta a todos los requisitos actuales de comunicación de un edificio; pero lo más importante es que se construye con la capacidad de adaptarse a nuevas necesidades a medida que éstas surjan.

El sistema de Cableado Estructurado debe ser capaz de transmitir información de múltiples protocolos y tecnologías e incorporar nuevos o futuros servicios a la red existente, sin perder la eficiencia ni el nivel de los servicios disponibles. Además, debe facilitar el manejo y administración de los servicios conectados.

Comparación entre Sistema de Cableado Estructurado y No Estructurado

Los sistemas tradicionales de cableado permiten los mismos servicios que un sistema estructurado. Sin embargo, las instalaciones están limitadas a una aplicación.

El Cableado Estructurado brinda la facilidad de usar un solo tipo de cable para todos los servicios de comunicaciones, lo que resulta en una total estandarización de la red.

Una característica bien conocida del cableado tradicional es que tiene poca capacidad de migración. No podemos cambiar fácilmente a un usuario de ubicación física, aunque sólo se desplace algunos metros, porque el cable no alcanza o el ducto de canalización está saturado. Situación que no ocurre en un sistema de Cableado Estructurado.

Por otro lado, el Cableado Estructurado es flexible, ya que permite planear el aumento de las capacidades y disminuye los costos en las actualizaciones o la ampliación de cableado para soportar nuevos servicios.

2.3 Componentes de un Sistema de Cableado Estructurado

Una instalación de Cableado Estructurado debe contar con toda la línea de productos, desde el tipo de cable a utilizar hasta los adaptadores terminales, que aseguren la conectividad y operación de cualquier tipo de aplicación.

Se entiende por aplicación, al diseño de ingeniería que define qué tipo de cable es el más adecuado para conectar un equipo o sistema (de cómputo, seguridad, control, telefónico, etc.), qué adaptadores se deben colocar para asegurar que las señales mantengan sus características técnicas, determinar las distancias máximas a las cuales se pueden conectar los equipos terminales, etc. Estos componentes son los siguientes:

- Medios de transmisión: Cables UTP o STP de 4 o 5 pares en diferentes categorías, cables multipar o cables de fibra óptica de diferentes tipos.

- Elementos de administración: Bloques de conexión (tipo 110) o paneles tipo RJ45 con sus elementos de fijación del cable y de organización del mismo.

- Cables preconectados para asignación de señales: Cables terminados en conectores tipo 110 de 1 a 4 pares; terminados en conector RJ45 en ambos extremos; Terminado en tipo 100 en un extremo y RJ45 en el otro y finalmente con conector tipo 110 o RJ45 en un extremo y cables sin conectar en el otro. En cuanto a fibra óptica, se encuentran cables preconectados con conectores ST, SC, bicónicos, etc., ya sea en ambos extremos o en combinaciones de manera similar con los cables de cobre. Se encuentran en fibra monomodo o multimodo. Con estos diferentes tipos de terminado, se realiza la administración del sistema.

- Adaptadores: Son los diferentes tipos de elementos que permiten integrar en un sistema de cableado, cualquier tipo de aplicación. Este es uno de los elementos importantes, pues aseguran que un sistema de cableado se comporte como un sistema abierto. Estos adaptadores aseguran que la señal transmitida entre los equipos a través del sistema de cableado se conserve balanceada y limpia.

- Protecciones para dispositivos y equipos: Dentro de los componentes que, por desconocimiento, muchas veces no se tienen en cuenta en los diseños, están las protecciones contra sobrevoltaje. Estas protecciones se requieren especialmente en soluciones que integren varias edificaciones. Los sistemas de protección controlan cada par de cable instalado. Existen diferentes tipos de fusible como son los de Gas o los de Estado Sólido. Paralelo al sistema de protecciones se debe contar con los polos a tierra adecuados y suficientes, que aseguren el funcionamiento y operación de las protecciones que se instalen.

- Sistemas de distribución del cableado: Otro punto importante a considerar son los elementos y materiales que aseguran una distribución técnica y adecuada del cableado a instalar. Aquí se

encuentran las canaletas o bandejas (en lámina o de aluminio), escalerillas, tuberías, etc. Adicionalmente, encontramos las cajas de terminación múltiples para cielo raso o piso falso y los accesorios con las curvaturas y capacidades exigidas por las normas.

Se debe tener en cuenta que el proveedor de un sistema de cableado cuente con la línea completa de productos, para asegurar que lleguen a instalarse en una aplicación, que estén debidamente probados en laboratorio y verificado su comportamiento de forma conjunta. En muchos casos, se hacen instalaciones en las cuales los componentes de una aplicación son suministrados por diferentes proveedores y, a pesar de que cada uno de estos componentes individualmente cumple con las normas aplicables, presentan fallas al funcionar como una aplicación completa.

2.4 Estándares Aplicables al Cableado Estructurado

Los sistemas de Cableado Estructurado deben emplear una Arquitectura de Sistemas Abiertos (OSA por sus siglas en inglés) y soportar aplicaciones basadas en estándares como el EIA/TIA 568-A, EIA/TIA 569, EIA/TIA 570, EIA/TIA 606, EIA/TIA 607 (de la Electronic Industries Association / Telecommunications Industry Association). Este diseño provee un solo punto para efectuar movimientos y adiciones de tal forma que la administración y el mantenimiento se convierten en una labor simplificada.

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de estos estándares de ANSI/TIA/EIA definen el cableado de telecomunicaciones en edificios. Cada estándar cubre una parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas. Cada estándar ANSI/TIA/EIA menciona estándares relacionados y otros materiales de referencia.

La mayoría de los estándares incluyen secciones que definen términos importantes, acrónimos y símbolos.

Los cinco estándares principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios son:

- ANSI/TIA/EIA 568-A, Estándar de Cableado de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA 569, Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA 570, Estándar de Alambrado de Telecomunicaciones Residencial y Comercial pequeño.
- ANSI/TIA/EIA 606, Estándar de Administración para la infraestructura de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-607, Requerimientos de Puesta a Tierra para Telecomunicaciones.

EIA/TIA 568-A Cableado de Telecomunicaciones en Edificios Comerciales

El estándar TIA/EIA 568-A define un sistema genérico de cableado de telecomunicaciones para edificios comerciales que soporten un ambiente de productos y múltiples proveedores. El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán.

El cableado de telecomunicaciones especificado en esta norma tiene por finalidad apoyar una gama muy amplia de diferentes edificios comerciales y de aplicaciones (por ejemplo, voz, datos y video).

El sistema de Cableado Estructurado descrito en el estándar TIA/EIA 568-A se basa en una topología de tipo estrella, la cual consiste en una conexión de ligas de punto a punto originadas en un Hub.

El estándar TIA/EIA 568-A enumera los siguientes seis elementos de un sistema de Cableado Estructurado:

I Subsistema Entrada del edificio.
II Subsistema Cuarto de equipo.
III Subsistema Cableado horizontal.
IV Subsistema Cuarto de telecomunicaciones.
V Subsistema Cableado vertical (Backbone).
VI Subsistema del área de trabajo.

En la Figura 2.12 se muestran los subsistemas de un Cableado Estructurado:

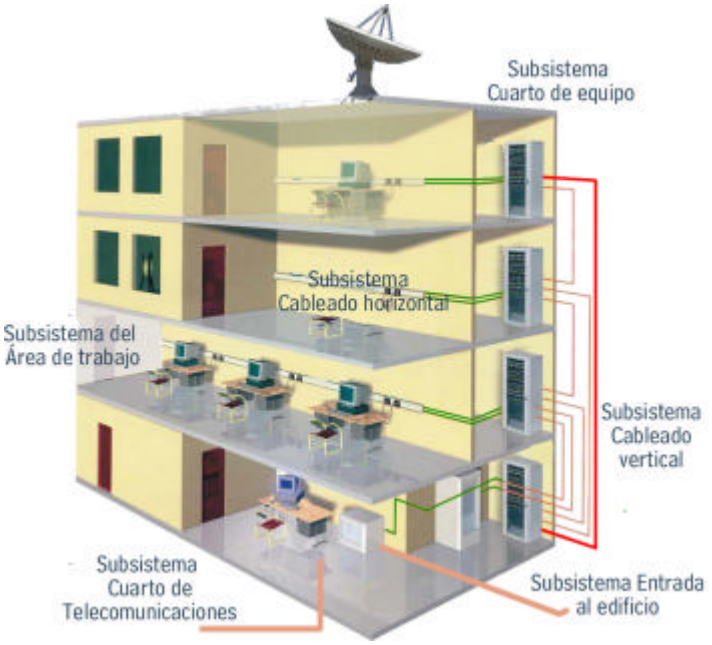


Figura 2.12 Subsistemas de un Sistema de Cableado Estructurado

I Subsistema Entrada del Edificio

La entrada del edificio provee el punto en el cual el cableado externo se une con el cableado vertical (backbone) interno del edificio. Los requerimientos físicos de dicha interfaz están definidos en la norma EIA/TIA 569 (Rutas y espacios de telecomunicaciones).

Este subsistema consiste en una entrada de servicios de telecomunicaciones al edificio, la cual incluye el punto de entrada a través de la pared del edificio y continuando al cuarto o área de entrada. La entrada al edificio debe contener la ruta del backbone que interconecta con los otros edificios; en caso de una comunicación a través de una antena, ésta también pertenece a la entrada del edificio.

Figura 2.13 Subsistema de Entrada al Edificio

II Subsistema Cuarto de Equipo

El cuarto de equipo es un espacio centralizado para los equipos de telecomunicaciones (Ej. PBX, equipos de cómputo, switch, etc.), que sirven a los ocupantes del edificio. Este cuarto, debe guardar únicamente equipos directamente relacionados con el sistema de telecomunicaciones y sus sistemas de soporte. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y la complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. De ahí que todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo.

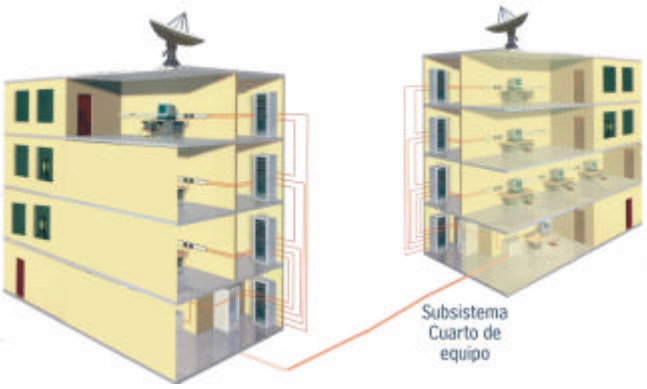


Figura 2.14 Subsistema Cuarto de Equipo

III Subsistema Cableado Horizontal

El cableado horizontal es la porción del sistema de cableado que se extiende desde el closet de telecomunicaciones (rack) hasta el usuario final en su estación de trabajo y consta de:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo.
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles y cables utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Las cuales proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones.

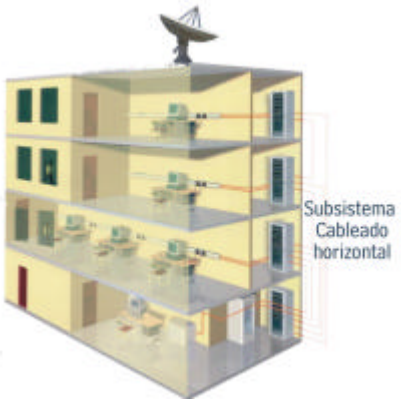


Figura 2.15 Subsistema de Cableado Horizontal

Consideraciones para el cableado horizontal

1. Distancias horizontales

La distancia horizontal máxima es de 90m, independiente del cable utilizado. Esta es la distancia entre el área de trabajo de telecomunicaciones y el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 m. adicionales para la distancia combinada de cables de empate (3 m.) y cables utilizados en la conexión de equipo en el área de trabajo y el cuarto de telecomunicaciones.

2. Tipos de cables

Existen tres tipos de cables utilizados en los sistemas de cableado horizontal:

- Cable UTP (Unshielded Twisted Pair).
- Cable STP (Shielded Twisted Pair).
- Fibra Óptica.

El cable más utilizado es el par trenzado sin blindaje UTP de cuatro pares.

3. Salidas del área de trabajo

Los ductos a las salidas del área de trabajo (work area outlet, WAO) deben proveer la capacidad de manejar tres cables. Las salidas de área de trabajo deben contar con un mínimo de dos conectores; uno de los conectores debe ser del tipo RJ-45, bajo el código de colores de cableado T568A ó T568B.

4. Adaptaciones comunes en el área de trabajo.

- Un cable especial para adaptar el conector del equipo (computadora, terminal, teléfono) al conector de la salida de telecomunicaciones.
- Un adaptador en "Y" para proporcionar dos servicios en un solo cable multipar (ej. teléfono con dos extensiones).
- Un adaptador pasivo utilizado para convertir el tipo de cable del equipo al tipo de cable del cableado horizontal.
- Un adaptador activo para conectar dispositivos que utilicen diferentes esquemas de señalización.
- Un cable con pares transpuestos.

5. Evitar la interferencia electromagnética

Al momento de establecer la ruta del cableado de los closets de cableado a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos, o al menos considerar las distancias sugeridas.

- Motores eléctricos grandes o transformadores (mínimo 1.2 m.).
- Cables de corriente alterna :
- Mínimo 13cm. para cables con 2KVA o menos.
- Mínimo 30 cm. para cables de 2KVA a 5KVA.
- Mínimo 91cm. para cables con más de 5KVA.
- Luces fluorescentes y balastros (mínimo 12 cm.).
- El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cm.).
- Equipo de soldadura.
- Aire acondicionado, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

IV Subsistema Cuarto de Telecomunicaciones

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de telecomunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que puedan existir en un edificio. Los cuartos de telecomunicaciones deben ser proyectados de acuerdo con los requerimientos del estándar ANSI/TIA 569.

Consideraciones de diseño:

El diseño de un cuarto de telecomunicaciones depende de:

- El tamaño del edificio.
- El espacio del piso a servir.
- Las necesidades de los ocupantes.
- Los servicios de telecomunicaciones a utilizarse.

Figura 2.16 Subsistema de Cuarto de Telecomunicaciones

V Subsistema de Cableado Vertical (Backbone)

El Subsistema de Cableado Vertical provee interconexión entre el cuarto de telecomunicaciones, cuarto de equipos y la entrada al edificio. Este consiste del cable backbone, del cable cruzado (cross-connect) intermedio y principal, de las terminaciones mecánicas y de los paneles de parcheo (patch cords).

El cuarto de equipo y los puntos demarcados pueden estar localizados en diferentes edificios; el backbone incluye los medios de transmisión entre diferentes edificios.

El cableado vertical debe soportar todos los dispositivos que están dentro del rack y a menudo todas las impresoras, terminales y servidores de archivos de un piso en un edificio. Si más clientes o servidores son agregados a un piso, ellos compiten por el ancho de banda disponible en el cableado vertical. Sin embargo existe una ventaja, y ésta consiste en la poca cantidad de canales verticales en

un edificio y por ello se pueden usar equipos más costosos para proveer un mayor ancho de banda. En donde la fibra óptica se ha convertido en el medio más apropiado. El cableado vertical se presenta en diferentes topologías, la más usada es la topología en estrella.

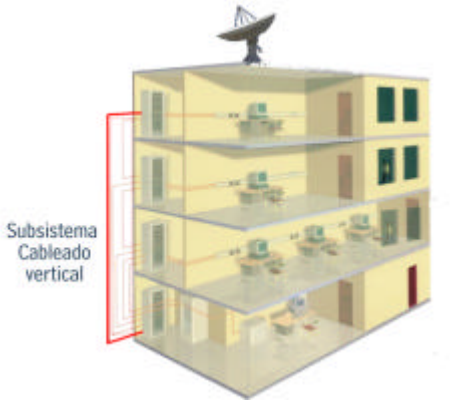


Figura 2.17 Subsistema de Cableado Vertical

Consideraciones al instalar el backbone:

1. Cables reconocidos ydistancias máximas

Cable	*Distancia (m)*	*Aplicación*
Cable UTP 100Ω	800	Voz y datos
Cable STP 150Ω	90	Datos
Cable multimodo de fibra óptica de 62.5/125 µm	3000	Datos
Cable monomodo de fibra óptica de 9/125 µm	2000	Datos

Nota. Las distancias del backbone, son dependientes de la aplicación. Las distancias máximas especificadas arriba se basan en transmisión de voz para UTP y en transmisión de datos para STP y fibra óptica

Tabla 2.2 Cables reconocidos y distancias máximas

2. Selección del medio de transmisión

Con cualquiera de los estándares existentes se puede construir un backbone para el cableado vertical; pero deben tenerse en cuenta los siguientes factores:

- Flexibilidad con respecto a los servicios soportados.
- Vida útil requerida para el backbone
- Tamaño del sitio y la población de usuarios.
- No se pueden colocar más de dos niveles jerárquicos de cross-connects.
- La longitud del patch-cord del cross-connect principal e intermedio no puede ser mayor a 20 m.
- El polo a tierra debe cumplir con los requerimientos definidos en la norma EIA/TIA 607 (Requerimientos de puesta a tierra para telecomunicaciones).

VI Subsistema del Área de Trabajo

El concepto de área de trabajo está asociado al concepto de punto de conexión. Comprende las inmediaciones físicas de trabajo habitual (mesa, silla, zona de movilidad, etc.) de los usuarios. El punto que marca su comienzo en lo que se refiere a cableado es la roseta o punto de conexión.

En el ámbito del área de trabajo se encuentran diversos equipos activos del usuario tales como teléfonos, computadoras, impresoras, telefax, terminales, etc. La naturaleza de los equipos activos condicionan el tipo de los conectores existentes en las rosetas, mientras que el número de los mismos determina si la roseta es simple (1 conector), doble (2 conectores), triple (3 conectores), entre otros.

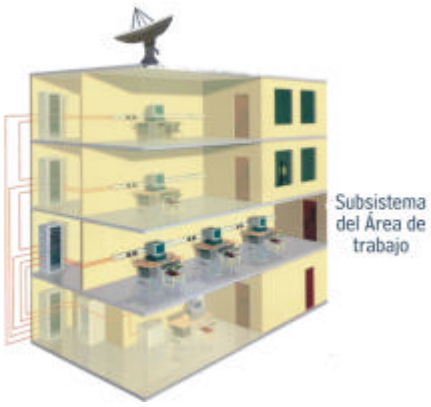


Figura 2.18 Subsistema del Área de Trabajo

EIA/TIA 569 Rutas y Espacios de Telecomunicaciones

El alcance de esta norma se limita al componente de telecomunicaciones relacionado con el diseño y construcción de edificios comerciales, abarcando problemas de telecomunicaciones de un edificio y entre edificios. Estos incluyen las vías o conductos en los cuales se encuentran localizados los medios de telecomunicaciones, así como los cuartos y áreas asociadas con el edificio usado para instalar equipos de telecomunicaciones

Este estándar reconoce un precepto de fundamental importancia: De manera que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

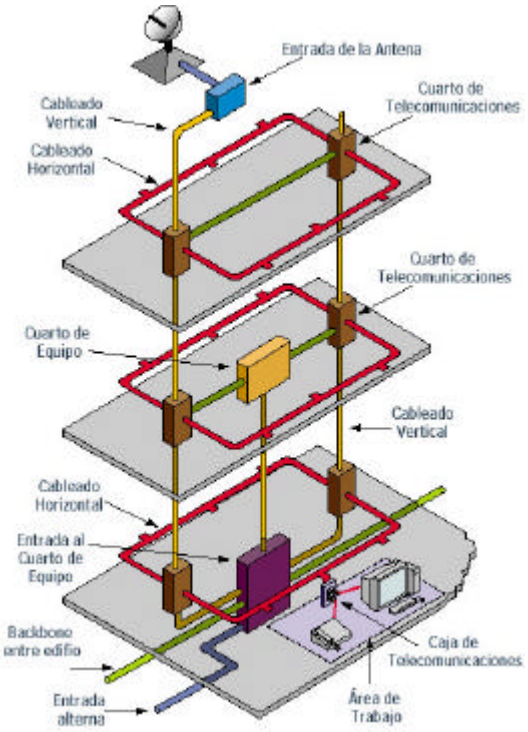


Figura 2.19 Subsistema del estándar EIA/TIA 569 de Cableado Estructurado

La aplicación de la presente norma en los subsistemas del Cableado Estructurado se menciona a continuación.

Subsistema Entrada del Edificio

Este subsistema consiste en una entrada de servicios de telecomunicaciones al edificio, que es el punto de acceso a través de la pared del edificio y continuando al cuarto o área de entrada. El ingreso al edificio debe contener la ruta del backbone que interconecta con los otros edificios; en caso de una comunicación a través de una antena, ésta también pertenece a la entrada del edificio.

Los puntos a considerar en la entrada del edificio son los siguientes:

- Localización del edificio.
- Vías de telecomunicaciones para la entrada de los servicios.

Subsistema Cuarto de Equipos

Los requerimientos del cuarto de equipos se especifican en los estándares ANSI/TIA/EIA 568-A (Cableado de telecomunicaciones) y ANSI/TIA/EIA 569 (Rutas y espacios de telecomunicaciones).

Para que un cuarto de equipo funcione adecuadamente, se deben tener en cuenta las siguientes consideraciones para el diseño.

- Selección del sitio
- Tamaño
- Aprovisionamiento
- Equipos de calefacción, ventilación y aire acondicionado
- Acabados interiores
- Iluminación
- Energía
- Puerta
- Polo a tierra
- Extinguidores de fuego

Subsistema Cableado Horizontal

Rutas y espacios horizontales
Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado horizontal.

El término horizontal es utilizado debido a que típicamente el sistema de cableado se instala horizontalmente a través del piso o del techo del edificio.

El cableado horizontal consta de cable par trenzado de cobre, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica.

Subsistema Cuarto de Telecomunicaciones

Consideraciones de diseño:

- Altura
- Ductos
- Puertas
- Polvo y electricidad estática
- Control ambiental
- Prevención de inundaciones
- Pisos
- Iluminación
- Localización
- Potencia
- Seguridad

Requisitos de tamaño
Debe haber al menos un cuarto de telecomunicaciones por piso y por áreas que no excedan los 1000 m2. Para que las instalaciones pequeñas puedan utilizar un solo cuarto de telecomunicaciones si la distancia máxima de 90m no se excede.

Disposición de equipos
Los racks deben de contar con al menos 82cm de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82cm se debe medir a partir de la superficie más la salida del rack.

Debe haber por lo menos 1m de espacio libre para trabajar de equipo con partes expuestas sin aislamiento.

Todos los racks y gabinetes deben cumplir con las especificaciones de ANSI/EIA.
Se recomienda dejar un espacio libre de 30cm, en las esquinas.

Subsistema Cableado Vertical (Backbone)

El número de puntos de conexión en una instalación (1 punto de conexión por área de trabajo) se determina en función de las superficies útiles o de los metros lineales de fachada, mediante la aplicación de la siguiente norma general; 1 punto de acceso por cada 8 a 10 metros cuadrados útiles o por cada 35 metros de fachada. Este número se debe ajustar en función de las características específicas del emplazamiento, por ejemplo, los locales del tipo de salas de informática, salas de reuniones y laboratorios.

En el caso que exista telefonía e informática, un dimensionado de tres tomas por punto de conexión constituye un criterio satisfactorio. Dicho dimensionado puede ajustarse en función de un análisis de necesidades concretas, pero no deberá, en ningún caso, ser inferior a dos tomas por punto de conexión del área de trabajo. Una de las tomas deberá estar soportada por pares trenzados no apantallados de cuatro pares y los otros por cualquiera de los medios de cableado.

Subsistema del Área de trabajo

La presente norma cubre aquellos aspectos de la estación de trabajo relacionados con salidas de telecomunicaciones.

Salidas de telecomunicaciones

Una salida de telecomunicaciones es el lugar del punto de conexión entre el cable horizontal y los cables que conectan aparatos en el área de trabajo, por ejemplo, los teléfonos, computadoras personales, etc.

Se debe instalar un mínimo de una salida por estación de trabajo. Para fines de planificación, el espacio disponible por estación de trabajo debe ser de 10 m2 en promedio. Para áreas de edificios en los cuales resulte difícil añadir salidas de telecomunicaciones futuras, en el diseño inicial se deben colocar un mínimo de dos salidas separadas para esa área; además, tales áreas deberán ser colocadas de modo que ofrezcan la máxima flexibilidad para cambios en el área de trabajo.

EIA/TIA 570 Alambrado de Telecomunicaciones Residencial y Comercial pequeño.

Este estándar da una visualización del cableado considerando los requerimientos de las especificaciones de instalación y de los componentes técnicos. Provee información para seleccionar las interfaces de los jacks, guías de instalación del cableado, descripción de los componentes y referencia, etc. El estándar EIA/TIA/ 570 es considerado como un complemento del estándar ANSI/TIA/EIA 568-A (Cableado de Telecomunicaciones en Edificios Comerciales).

Este estándar describe el cableado de los sistemas considerando la conexión con uno o varios accesos de línea para varios tipos de equipo. Define un sistema de cableado genérico y funcional para telecomunicaciones donde la construcción del edificio soporte multiproductos. La instalación del sistema de cableado debe ser durante la construcción del edificio, puesto que el realizar esto, permite que sea menos costoso, que después de ser ocupado el edificio.

EIA/TIA 606 Administración para la Infraestructura de Telecomunicaciones

Este estándar especifica los requerimientos de administración de la infraestructura, ya sea un edificio nuevo, existente o renovado. La infraestructura de telecomunicaciones puede ser ideada como la conexión de varios componentes: espacio del equipo de comunicaciones, ruta del cable, sistema de tierra físico, cableado y la terminación al hardware, que provee el soporte básico de la distribución de toda la información dentro de un edificio. La administración de telecomunicaciones incluye la documentación de las cajas de conexión, conectores, terminación del hardware, conexión, tubo conduit, otro tipo de rutas del cable, closets de telecomunicaciones, y otros espacios.

El propósito de este estándar es proporcionar un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. Este estándar establece guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

Los edificios modernos requieren una efectiva infraestructura de telecomunicaciones para soportar la variedad de servicios que dependen del transporte electrónico de la información. La administración incluye documentación básica y los planos actualizados, etiquetado y registros. La administración debe contemplar datos, voz y video, así como con otros sistemas del edificio: por ejemplo, seguridad, audio, alarmas y energía. La administración puede ser acompañada de registros en papel y de sistemas en computadora.

Conceptos de administración

El típico sistema de administración incluye: registros, reportes, esquemas y registros de trabajo.

Identificadores. Cada espacio, ruta, punto terminal del cable y tierra, debe ser asignado a un solo número de identificación, el cual, debe ser un código simple.

Los identificadores pueden clasificarse como:
Identificadores de ruta.

a) CT Bandeja de entrada.
b) CD Conducto.
c) BCD Conducto de Backbone.

Identificadores de espacio.

a) EF Infraestructura de entrada.
b) ER Sala de equipos.
c) IC Conexión cruzada intermedia.
d) HH Orificio de acceso.
e) S Empalme.

Identificadores de cable.

a) C Cable.
b) CB Cable de "backbone".
c) F Fibra.

Identificadores de conexión a tierra

a) BC Conductor unión.
b) EC Conductor de equipo.
b) GB Barra de distribución de tierra.
c) TGB Barra de distribución de tierra de telecomunicaciones.
d) TMGB Barra de distribución de tierra principal de telecomunicaciones.

Registros de telecomunicaciones. Mínimo se requieren registros por cable, espacio, ruta, tierra física y terminación del hardware. Estos registros permiten ligar información a otros reportes.

Los registros de telecomunicaciones se clasifican en:

a) Registros de ruta.
b) Registros de cable.
c) Registros de espacio.

d) Registros de conexión a tierra.
e) Registros de posición de terminación.

Reportes opcionales. Pueden existir registros de otros dispositivos, como pueden ser: PBX, inventario de equipo (teléfonos, PCs) e información de los usuarios (extensión, ubicación, etc.).

Dibujos. Dibujos que incluyan planos de los pisos, ruta del cableado y esquemas de los racks.

Orden de trabajo. Orden de trabajo que incluye espacios, rutas de los cables, sistema de tierra. La orden de trabajo debe listar las responsabilidades para cambios físicos, así como la actualización de la documentación para futuros cambios.

Formatos de identificación. Un solo código de identificación alfabética debe ser creado por cada lugar, ruta de cable, punto terminal.

De cualquier forma, el escoger un formato debe ser considerado y proveer un solo número de identificador para cada elemento del sistema. Este método permite por sí mismo organizar y actualizar los múltiples registros en uso, logrando un programa de base de datos.

EIA/TIA 607 Requerimientos de Puesta a Tierra para Telecomunicaciones

Con el incremento en el empleo de sistemas de cómputo y telecomunicaciones más sofisticados, veloces y sensibles, se ha hecho necesario y fundamental contar con sistemas de suministro de energía más confiables y seguros. Una parte fundamental para la adecuada operación de las instalaciones eléctricas, es el buen diseño de dichas instalaciones, así como la correcta instalación, operación y manipulación de los equipos que operan con energía eléctrica.

El progreso en la comunicación de voz y datos y su convergencia, ha permitido cada vez más interactuar con los propios sistemas complejos. Estos sistemas requieren de un sistema de tierra física confiable.

Para llegar a cumplir con este objetivo, cada país ha formulado un conjunto de normas, las cuales tienen la finalidad de establecer especificaciones de carácter técnico y de seguridad para sus instalaciones eléctricas, teniendo como objetivo principal proteger la vida de las personas, y de los equipos electrónicos.

Esta norma regula las especificaciones sobre los sistemas de tierra para equipos de telecomunicaciones. La conexión a tierra en las instalaciones eléctricas se realiza mediante el sistema de tierra, cuyo funcionamiento primordial es conducir hacia tierra (subsuelo) todas aquellas corrientes de cualquier naturaleza, corrientes de falla, frecuencias indeseables o descargas atmosféricas.

El sistema de tierra se compone de un conjunto de conductores interconectados entre sí y conectados a tierra mediante electrodos enterrados a cierta profundidad en el subsuelo. Los componentes principales que forman el sistema de tierras son los electrodos de puesta a tierra.

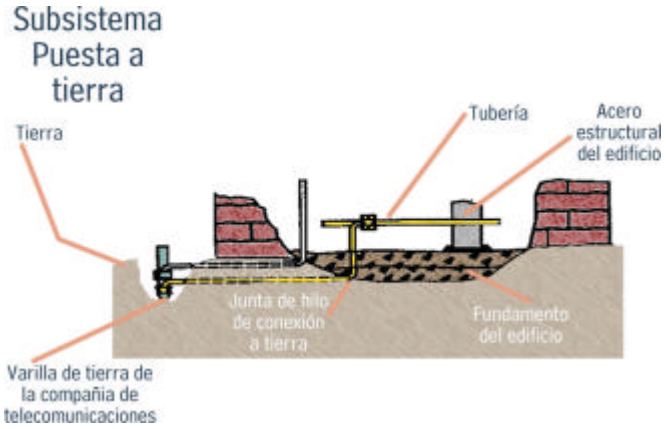


Figura 2.20 Subsistema Puesta a Tierra

Consideraciones de diseño.

Las varillas sólidas de cobre deben ser instaladas a una distancia lejana de la entrada al edificio, las varillas pueden ser de (1/4" de delgada por 4" de altura, por longitud variable); cuarto de equipo, cada closet de telecomunicaciones (2" de altura es suficiente aquí).

El equipo de telecomunicaciones, gabinetes, racks y los protectores de voltaje son típicamente aterrizados al sistema de tierra fisco. Las varillas son conectadas por un backbone con aislamiento, cable de cobre sólido entre todos los closets y cuartos de equipos (mínimo 6 AWG, 3/0 AWG recomendado). Este backbone es conectado a la principal varilla en la entrada del edificio a un sistema de tierra física en la entrada del edificio, y una estructura de acero en cada piso, vinculando el conductor del cable de color verde o con un etiquetado apropiado.

Las principales funciones que debe cumplir todo sistema de tierra son las siguientes:

a) Proveer un medio seguro para proteger al personal y al equipo de los peligros de una descarga eléctrica bajo condiciones de falla.

b) Proporcionar un circuito de mínima impedancia para la circulación de las corrientes de falla, debidas a condiciones anormales de operación.

c) Evitar que durante la circulación de estas corrientes a tierra, se produzcan diferencias de potencial entre los diversos equipos puestos a tierra.

d) Evitar la inducción de ruido en los equipos de telecomunicaciones.

La puesta a tierra de sistemas, circuitos, equipos, canalizaciones y cubiertas metálicas debe ser permanente y continua, los elementos que la constituyen deben tener una capacidad suficiente para conducir cualquiera de las corrientes originadas en disturbios y ser de impedancias suficientemente baja para evitar diferencias de potencial que puedan dañar los equipos y al personal, y para facilitar el funcionamiento de los dispositivos de protección contra sobrecorriente del circuito.

La puesta a tierra consiste básicamente en conectar a tierra las partes metálicas no conductoras de corriente, que alojan a los sistemas o aparatos que utilizan, cajas de registro, gabinetes metálicos, estructuras que soportan equipo eléctrico, carcazas de motores, tanques metálicos de transformadores, en general, todas las estructuras metálicas.

El sistema de puesta a tierra para una instalación de telecomunicaciones está constituido por cinco componentes principales:

1. Sistema de Electrodos de Tierra o Mallas de Tierra.
2. Barra principal de Tierra.
3. Cable Vertical
4. Barra de Tierra
5. Ventana de Tierra

Estos cinco componentes proveen la base para el diseño de la trayectoria de puesta a tierra a los equipos.

Norma de Cableado Estructurado en México

La Norma Mexicana NMX-I-248-1998-NYCE (Telecomunicaciones -Cable Estructurado -Cableado de Telecomunicaciones para Edificios Comerciales -Especificaciones y Métodos de Prueba) establece los requisitos mínimos aplicables al cableado de telecomunicaciones dentro de un edificio, hasta la salida/conector de telecomunicaciones y entre edificios en un ambiente de campus. El Cableado Estructurado especificado por esta norma aplica una amplia variedad de localidades para edificios comerciales por ejemplo, voz, datos, texto, video e imágenes. Esto incluye localidades con una extensión geográfica de hasta 3,000m y hasta 1,000,000m2 de espacio de oficinas con una población de hasta 50,000 usuarios individuales.

Esta norma mexicana establece los requerimientos mínimos que debe cumplir un sistema de cableado genérico para telecomunicaciones en edificios comerciales, que soporte un ambiente de múltiples productos y proveedores, especificando los requerimientos de los componentes, las distancias del cableado, las configuraciones de salida/conector de telecomunicaciones y la topología recomendada.

Los elementos de la estructura del sistema de Cableado Estructurado de telecomunicaciones comprendidos en esta norma son los siguientes:

a) Cableado horizontal.
b) Cableado vertical (backbone).
c) Área de trabajo.
d) Cuarto de telecomunicaciones.
e) Cuarto de equipo.
f) Instalaciones de acometida.
g) Administración.

Cableado horizontal

El cableado horizontal incluye los cables horizontales, la salida/conector de telecomunicaciones en el área de trabajo, la terminación mecánica y los cables de parcheo o puentes ubicados en el cuarto de telecomunicaciones.

Dicho cableado debe aumentar equipo futuro y cambios en el servicio; contiene la mayor cantidad de cables individuales en el edificio. Una vez construido el edificio, el cableado horizontal generalmente es menos accesible que el cableado vertical, y por lo tanto, el tiempo, el esfuerzo y las habilidades requeridas para efectuar los cambios, pueden ser extremadamente altos. Así mismo, el cableado horizontal debe ser de una topología de tipo estrella.

Para cables de fibra óptica, es aceptable cualquier combinación de longitudes entre el cableado horizontal y los cordones de área de trabajo y de parcheo, sin que ésta exceda los 100m.

La distancia horizontal debe ser de 90m, independientemente del tipo de medio, esto es, la longitud del cable desde la terminación mecánica del medio.

Esta norma reconoce tres cables para uso en el sistema de Cableado Estructurado en el cableado horizontal:

- Cables de par trenzado sin blindaje (UTP).
- Cable de par trenzado con pantalla (FTP).
- Cable de fibra óptica.

Esta norma reconoce la importancia de las telecomunicaciones de voz y de datos en un edificio. Se debe proporcionar un mínimo de dos salida/conectores de telecomunicaciones, por cada área de trabajo individual.

Cableado Vertical

La función del cableado vertical es proporcionar interconexiones entre los cuartos de telecomunicaciones, los cuartos de equipo y las instalaciones de acometida en la estructura del

sistema de cableado de telecomunicaciones. El cableado vertical consiste de cables verticales, conexiones, terminaciones mecánicas y cables de parcheo o puentes utilizados. El cableado vertical incluye el cableado entre edificios.

El cableado vertebral debe utilizar la jerarquía convencional para la topología de estrella. Si se anticipan los requerimientos para configuraciones de "bus" o "anillo" se permite el cableado directo entre los armarios de telecomunicaciones, dcho cableado es adicional a las conexiones para la topología de estrella básica.

Área de Trabajo.

Los componentes del área de trabajo se extienden desde el extremo de salida/conector de telecomunicaciones del sistema del cableado horizontal, hasta el equipo de la estación y está fuera del alcance de esta norma. El equipo de la estación puede diversos dispositivos que incluyen, pero no se limitan a los teléfonos, terminales de datos y computadoras. El cableado del área de trabajo es crítico para un sistema de distribución bien administrado; sin embargo, generalmente no es permanente y está diseñado para que su cambio sea relativamente sencillo. Por lo tanto, no se incluye en esta norma una especificación por separado del cableado en el área de trabajo.

Cuartos de Telecomunicaciones

Los cuartos de telecomunicaciones proporcionan muchas funciones distintas para el sistema de cableado y generalmente son tratados como un subsistema diferente de cableado jerárquico.

La función principal de un cuarto de telecomunicaciones es la terminación del cable de distribución horizontal. Los cables horizontales de todos los tipos reconocidos se determinan en el cuarto de telecomunicaciones en accesorios de conexión compatibles.

Cuartos de Equipo

Los cuartos de equipo se consideran distintos a los cuartos de telecomunicaciones; en la presente norma, debido a la naturaleza o complejidad del equipo que contienen. Cualquiera de las funciones de un cuarto de telecomunicaciones puede ser proporcionada por un cuarto de equipo.

Un cuarto de equipo proporciona un ambiente controlado para albergar equipo de telecomunicaciones, accesorios de conexión, cámaras, aparatos de protección que sean necesarios, etc.

Instalaciones de acometida

Las instalaciones de acometida consisten en cables, accesorios de conexión, dispositivos de protección y el equipo necesario para conectar las facilidades de planta externa al cableado local. Estos componentes pueden ser utilizados por los servicios de la red pública, servicios locales de la

red privada del cliente, o ambos. El punto de demarcación entre los portadores/proveedores de servicios regulados y el cableado local del cliente, puede ser parte de la instalación de acometida.

Las instalaciones de acometida incluyen las conexiones entre el cableado utilizado en el ambiente externo y el cableado autorizado para la distribución dentro del edificio.

Administración

Las salidas multiusuario se deben administrar de la misma forma que el cableado, los accesorios de conexión, las vías y los espacios descritos en la especificación particular.

El cable del área de trabajo que conecta la salida multiusuario con el equipo, debe ser etiquetado, en ambos extremos con un identificador único. El extremo del cable del área de trabajo que se conecte a la caja multiusuario, debe ser etiquetado con el identificador del área de trabajo a la que sirve, y el extremo que conecta al área de trabajo con el identificador correspondiente a la caja multiusuario y al puerto al que se conecta.

2.5 Aspectos Importantes en el Diseño de Cableado Estructurado

Con el objeto de generar un método amplio para el diseño del Cableado Estructurado es necesario que el diseñador posea la información completa de todo el proyecto.

Algunos aspectos que ayudan a identificar el tipo de información que se debe recopilar, son:

- Conocer las necesidades actuales del usuario (voz, datos, video y otros).
- Considerar las necesidades futuras del usuario (expansión en voz, datos, video, etc.).
- Conocer el tipo de construcción del lugar.
- Contemplar el tipo de estructura que se está utilizando (muros o lozas).
- Localizar los puntos de los servicios.
- Identificar los requerimientos especiales para la colocación de los servicios.

Una lista de los factores que hay que considerar en el momento de especificar un sistema de cableado son:

- La estrategia en tecnologías de información de la empresa o institución.
- Si el área que va a ser cableada es nueva, está en fase de remodelación o va a estar operando durante la instalación.
- Considerar el número de personas a las cuales se les va a dar soporte con el nuevo cableado.
- Servicios que debe soportar por puesto individual.
- Localización, diseño, tamaño y tipo de los edificios o plantas involucradas.
- Grado de integración con los equipos actuales.

- Espacios existentes en techos, suelos y verticales para el tendido del cableado horizontal y vertical, respectivamente.
- Disponibilidad de espacio para la localización de armarios y equipos de comunicaciones.
- Permanencia de tiempo previsto en el edificio.
- Número probable de reubicaciones y cambios de distribución del personal en el edificio.
- Requisitos de seguridad.
- Costos del cableado y su instalación.
- Procedimientos de mantenimiento.

Recomendaciones al cablear

Para asegurar un alto desempeño en un cableado, y a fin de asegurar que los componentes estén instalados correctamente (es decir, de acuerdo con las prácticas reconocidas en la industria), se deben considerar los siguientes aspectos que las normas y estándares internacionales prevén al momento de cablear:

1. Considerar que la máxima longitud permitida para un cable UTP horizontal no debe exceder 90 metros, desde el cuarto de telecomunicaciones hasta el área de trabajo.
2. Al configurar el cuarto de telecomunicaciones se debe determinar cuál es el sitio más adecuado, qué tamaño se le asignará, y qué número de puertos se requieren. Esto facilitará futuras adiciones, movimientos y cambios en el sistema de Cableado Estructurado.
3. Trazar la ruta del cable, considerando el método de distribución más apropiado (falso plafón, piso falso, tubería ahogada -en piso, techo o muro- o canalización aparente).
4. Cuando se esté instalando cable categoría 5, el destrenzado de los conductores individuales deberá mantenerse dentro de media pulgada del punto de conexión. El destrenzar los conductores a más de esta distancia en el punto de conexión ocasiona diafonía.
5. La tensión de jalado permitida cuando se está instalando un cable UTP de cuatro pares es de 110 N (25 libras-pie), que previene una sobretensión del cable. Tensionar en exceso al jalarlo provoca estiramiento de los conductores y aplastamiento del cable, lo cual puede incrementar la atenuación y la diafonía en el segmento del cable.
6. El radio de curvatura durante y después de la instalación de un segmento de cable deberá ser respetado para asegurar el desempeño del cableado. Los requerimientos para el radio de curvatura son: cuatro veces el diámetro de un cable horizontal y 10 veces el diámetro de un cable vertical.
7. Considerar la distancia de separación con las fuentes de interferencia electromagnética (e.g balastros) y la energía eléctrica de un sistema puede degradar el desempeño de un sistema de cableado.
8. Espaciamiento de ductos. Las secciones del conducto no deberán ser más largas que 30.5 m, y la curvatura mínima deberá ser de 90 grados.

Recomendaciones en cuanto a canalizaciones y ductos.

1. Los cables UTP no deben circular junto con cables de energía dentro del misma ducto por más corto que sea el trayecto.
2. Debe evitarse el cruce de cables UTP con cables de energía. De ser necesario, éstos deben realizarse a 90 grados.
3. Los cables UTP pueden circular por bandeja compartida con cables de energía respetando el paralelismo a una distancia mínima de 10cm. En caso de existir una división metálica puesta a tierra, la distancia se reduce a 7cm.
4. En el caso de pisoductos o ductos metálicos, la circulación puede ser en conductos contiguos.
5. Si es inevitable cruzar un gabinete de distribución con energía, no debe circularse paralelamente a más de un lateral.
6. De utilizarse ducterías plásticas, se deberán lubricar los cables con (talco industrial, vaselina, etc.) para reducir la fricción entre los cables y las paredes de los ductos, ya que ésta genera un incremento de la temperatura y provoca un aumento en la adherencia.
7. El radio de las curvas no debe ser inferior a 5cm.
8. Al utilizar fijaciones (grapas, precintos o cinchos) no excederse en la presión aplicada (no arrugar la cubierta), ya que puede afectar a los conductores internos.

Costos en un sistema de Cableado Estructurado

Un importante factor diferenciador es el costo de cada solución. En la actualidad existe una amplia gama de suministradores de sistemas de Cableado Estructurado, todos ellos con características técnicas similares.

Los costos involucrados en un proyecto de cableado se pueden agrupar en las siguientes categorías:

- Ingeniería.
- Materiales (cables, rosetas, repartidores, etc.).
- Dirección de obra. Tendido y puesta en funcionamiento.
- Certificación final.
- Mantenimiento.

Los costos de instalación de un nuevo sistema de cableado son elevados debido a las altas inversiones en materiales y costos de mano de obra del tendido y de la obra civil requerida. Los Sistemas de Cableado Estructurado requieren mayores inversiones que sistemas no estructurados debido fundamentalmente a su topología en estrella y el sobredimensionamiento propio de cualquier precableado.

Un parámetro adecuado para comparar distintas ofertas es el costo por puesto, que se obtiene dividiendo el costo total de instalación entre el número de tomas dimensionadas.

La mayor ventaja de los sistemas de Cableado Estructurado respecto de las soluciones no estructuradas se encuentra en las labores de mantenimiento. En una solución estructurada, en la mayoría de los casos, el alta de un nuevo puesto se limita a realizar las conexiones adecuadas en el repartidor de planta.

Como regla general, la dirección de obra debe ser realizada por personal ajeno a la empresa instaladora. Esta figura será responsable de la dirección de proyecto, así como de la gestión de las posibles variaciones que fueran necesarias durante la instalación.

Los sistemas de Cableado Estructurado tienen un amplio rango de niveles de precio para el costo inicial y el costo real a largo plazo, con respecto a la vida del sistema. El precio inicial que se paga, no es igual al gasto total de un sistema de cableado.

La mayoría de los problemas que se tienen en las redes (60 a 70%) se localizan en la capa física del modelo OSI; es decir, que generalmente los problemas nunca están relacionados con el software. Normalmente se trata de una terminación incorrecta, una conexión inadecuada, interconexiones inapropiadas, conectores equivocados, cable cortado, malas características eléctricas de cable, etc.

CAPÍTULO 3

ANTECEDENTES Y ESTADO ACTUAL DE LA RED DE DATOS DE LA DEPFI.

En el presente capítulo se hace una recopilación de información acerca del entorno de la Red de Datos de la DEPFI y que es el contexto en el que se sitúa la red de datos actualmente.

En la primera sección se describe la trayectoria de la Red de Datos de la UNAM hasta la actualidad, en donde se mencionan los avances tecnológicos y los servicios que brinda a la Comunidad Universitaria. Se hace una descripción de la infraestructura del backbone actual.

Se recopiló información de los antecedentes de la Red de Datos de DEPFI, así como de la relación con la Facultad de Ingeniería (FI). Además, se presenta un resumen del documento que la FI elaboró, con el fin de poder reducir el número de incidentes presentados en el uso de la Red de Datos de la Facultad.

Finalmente se elaboró un resumen de los aspectos importantes de la Red de Datos de DEPFI, que serán la base para desarrollar el capitulo siguiente.

3.1 REDUNAM

La implantación de la red de la Universidad Nacional Autónoma de México (UNAM) tuvo sus inicios al final de la década de los 60 y principios de los 70. Este tipo de comunicaciones en la UNAM se llevó a cabo por medio de teletipos conectados a una computadora central. En este período también se comenzó la instalación de un tendido de líneas telefónicas de cobre, mediante el cual fueron conectados los teletipos. Con estas nuevas instalaciones la institución se comenzó a proporcionar servicio de conexiones para hacer uso de impresión e interconexión entre algunas estaciones de trabajo.

Debido a los cambios tecnológicos que se estaban dando en el mundo, en 1987 se realiza la primera conexión a la Red Académica de C o BITNET. Esta conexión se realizó entre la UNAM (en Ciudad Universitaria) y el ITESM para lograr una conexión con la ciudad de San Antonio, Texas, EUA. Cabe resaltar que para esta conexión se siguió empleando la línea telefónica de cobre existente.

En 1989, la UNAM establece un enlace con la red NSF en Colorado, EUA, con el apoyo del Instituto de Astronomía de esta institución. Para este enlace se hizo uso del satélite Morelos II. A partir de esa exitosa comunicación, se empezaron a dar los orígenes de las conexiones de redes de áreas locales (LAN´s). Primeramente por parte del Instituto de Astronomía y la Dirección General de Servicios de Cómputo Académico (DGSCA). Asimismo, se inicia la instalación y uso de fibra óptica dentro del campus universitario. Este hecho marca el comienzo de las telecomunicaciones dentro de la UNAM.

Empezó a surgir el "boom" de las LAN´s dentro de la UNAM, principalmente dentro de los institutos de investigación científica. El alto crecimiento que se comenzó a dar durante este período permitió desarrollar la infraestructura de comunicaciones con fibra óptica. De igual forma se hizo uso de enlace de microondas de alta velocidad. Éstos se hicieron entre la Torre II de Humanidades y la DGSCA. Estos logros alcanzados permitieron extenderse a instalaciones de la UNAM, fuera Ciudad Universitaria, por lo que se establecieron enlaces satelitales con Cuernavaca y San Pedro Mártir.

En este mismo año, se comenzó la sustitución de los conmutadores existentes por equipos con mayores capacidades, acordes con el avance tecnológico de ese entonces. El objetivo fue renovar el sistema telefónico de la UNAM. Se crea la Dirección de Telecomunicaciones Digitales (DTD), como parte del Programa Institucional en Informática, cuyo objetivo sería la creación de la Red Integral de Telecomunicaciones de la UNAM, la cual debería ser capaz de transmitir indistintamente datos e imágenes entre las dependencias universitarias, independientemente de su ubicación geográfica.

En 1990 la UNAM fue la primera institución en Latinoamérica que se incorpora a la red mundial Internet. Se crea el Laboratorio de REDUNAM, espacio dedicado a la investigación, estudio y análisis de la red de datos de la UNAM, así como del diseño de las redes futuras, uso de protocolos, servicios, etc.

La Red Integral de Telecomunicaciones de la UNAM se inaugura oficialmente en 1992; entre sus principales características destacan hoy en día:

- La transmisión indistinta de datos y video, mediante sistemas digitales basados en normas internacionales que rigen actualmente.

- La integración a la red de las principales instalaciones de la Universidad.

El proceso de evaluación de nuevas y diversas tecnologías da inicio a finales del año 1995, cuando la Dirección de Telecomunicaciones de la DGSCA inicia su labor de investigación. Posteriormente, realiza contacto con diferentes fabricantes para observar los productos disponibles y conocer el estado de madurez en el que se encuentra el desarrollo de dichas tecnologías.

Durante el primer semestre de 1996 el Forum ATM trabaja fuertemente en el desarrollo de múltiples estándares que muestran la madurez de la tecnología. Al mismo tiempo, el personal de la Dirección de Telecomunicaciones identifica la convergencia tecnológica de los equipos y sistemas de voz, datos y video en diferentes plataformas, dentro de las cuales, ATM es la que cubría con las necesidades y requerimientos de la UNAM.

Uno de los grupos especializados de trabajo de la Dirección de Telecomunicaciones inicia las actividades de diseño de la Red Integral de Telecomunicaciones con tecnología ATM. La operación de la Red Integral de Telecomunicaciones con una plataforma de backbone basada en la tecnología ATM (Figura 3.1) da inicio el mes de agosto de 1997. En ese año sólo se envía tráfico de datos. Posteriormente se incorporó el tráfico de voz y videoconferencia.

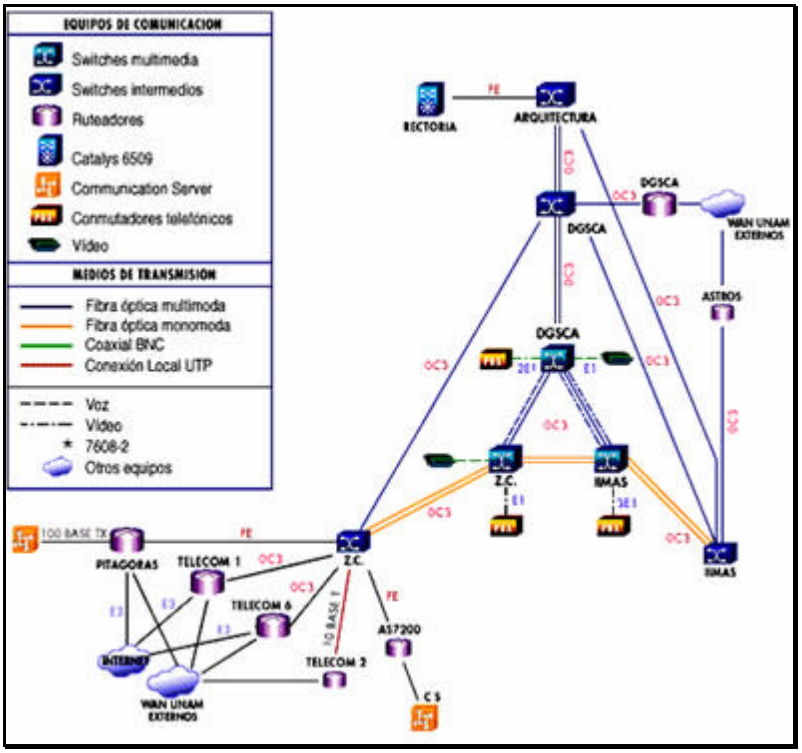


Figura 3.1 Backbone ATM de la UNAM

Actualmente, la UNAM cuenta con la Red Educativa ATM de Telecomunicaciones más grande de América Latina, así como con un grupo especializado de trabajo de alto nivel que se encarga de administrar, operar y controlar la infraestructura.

El proyecto del NOC (Network Operation Center) de la UNAM surge en mayo de 1996, incorporando a personal con sólidos conocimientos en la administración de redes y diversos temas de telecomunicaciones. El NOC cuenta con sistemas automatizados que verifican el estado de los dispositivos más importantes que forman el Backbone y recolectan información que posteriormente será procesada para su análisis.

En 1998 el puente entre la UNAM y la Escuela Permanente de Extensión en San Antonio, Texas (EPESA) ya cuenta con el enlace dedicado con la Universidad de Texas A&M (TAMU) en College Station. Oficialmente, a partir del 25 de junio, la UNAM forma parte de la Red TTVN (Trans Texas Video Network) que tiene acceso a más de 100 salas en los 13 campus de TAMU, además de otras universidades y escuelas. La EPESA se erige como puente académico y científico entre la UNAM y universidades de Estados Unidos y Europa. Actualmente se imparten simultáneamente cursos de inglés y español en todos los niveles; organizando seminarios, simposios, mesas redondas, conferencias, exhibiciones culturales, ferias de libros y proyecciones de películas. A través de una sofisticada instalación de satélites, la UNAM se conecta desde este polo de desarrollo académico y cultural, con más de 27 universidades estadounidenses y 7 del viejo continente, colocándose a la vanguardia educativa en el desarrollo de cursos fijos y videoconferencias.

El 8 de abril de 1999 se oficializó la constitución de la Corporación Universitaria para el Desarrollo de Internet (CUDI). La UNAM participó como miembro fundador de la CUDI y es una de las ocho Universidades asociadas. La Misión de CUDI es promover y coordinar el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México. Las actividades que se desarrollen deberán ser congruentes con los fines de las instituciones académicas que lo integran y con los servicios que éstas presten a la sociedad.

Como parte de las actividades de innovación y prospección en materia de redes de alto desempeño, la Dirección de Telecomunicaciones participa activamente en CUDI, como integrante del grupo de trabajo de diseño de la red nacional Internet 2. Al mismo tiempo mantiene su liderazgo en trabajos, como IPv6, QoS, Multicast, y redes inteligentes de almacenamiento, entre otros proyectos.

Igualmente, la UNAM se mantiene a la vanguardia mundial en cuestiones de redes de datos de altas capacidades, que son empleadas en aplicaciones de alta tecnología e investigación, al participar en la red internacional Internet2 (I2).

El backbone de I2 de la UNAM (Ver Figura 3.2) es capaz de soportar, de forma óptima, todos los servicios de datos, voz y video sobre IP y aplicaciones emergentes que se demanden; además es suficientemente flexible para permitir el crecimiento cuando se requiera.

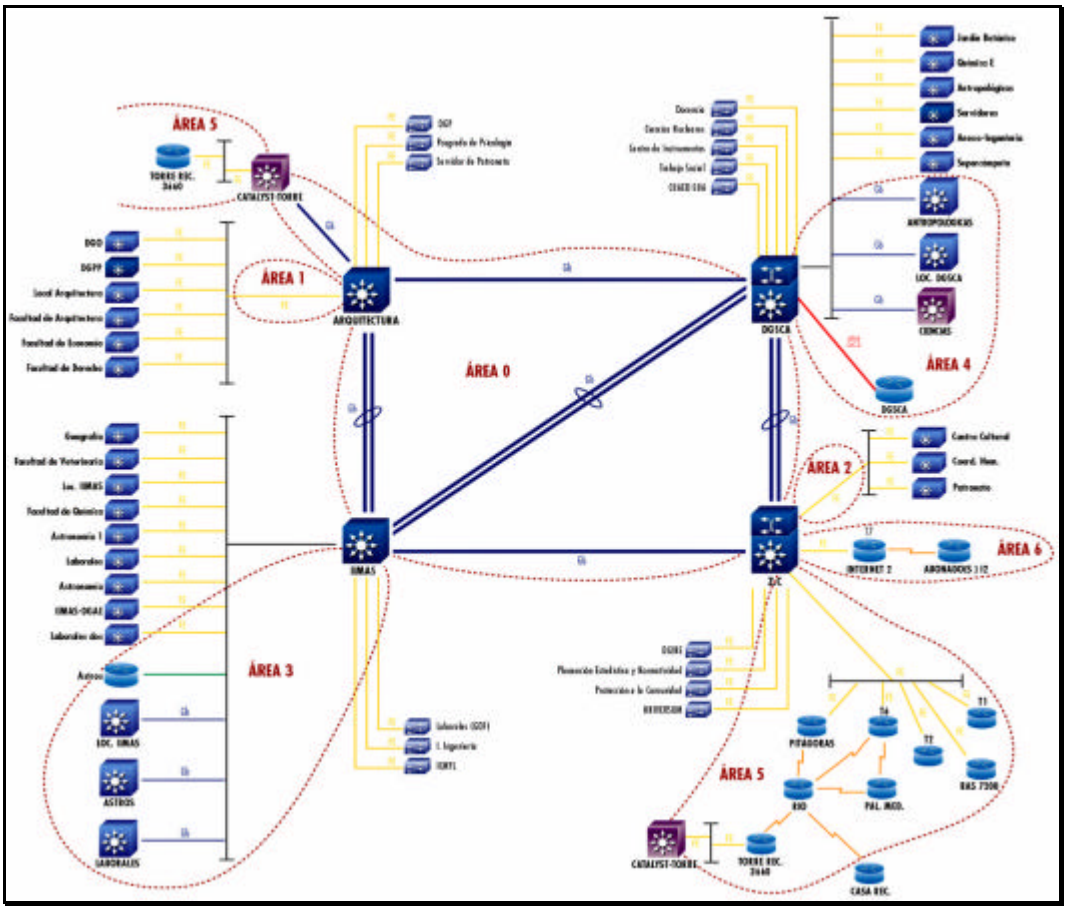


Figura 3.2 Backbone de I2 de la UNAM

"Cerca del 95% de los miembros de la UNAM se encuentran en instalaciones cubiertas por REDUNAM (incluyendo las sedes fuera de la Ciudad de México). El sistema está conformado por 32 nodos operacionales de telefonía, enlazados entre sí mediante fibra óptica, enlaces satelitales y de microondas. Posee una infraestructura instalada para 13,000 servicios telefónicos, alimentados por 2,400 troncales digitales conectadas vía fibra óptica con las centrales telefónicas públicas.

"Adicionalmente, la UNAM cuenta con una red complementaria de respaldo de más de 1,000 servicios, basada en telefonía celular y 17 líneas telefónicas directas. También cuenta con más de 600 redes locales en ocho regiones del país. La red enlaza a cerca de 10,000 computadoras de la UNAM entre sí y alrededor de 15 millones de computadoras en el resto del mundo.

"La UNAM a través de la DGSCA promueve y coordina el desarrollo de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo en México. Las actividades que se desarrollan son consistentes con los fines de las instituciones académicas que la integran y con los servicios que éstas prestan a la sociedad:

- Promover la creación de una red de telecomunicaciones con capacidades avanzadas.

- Fomentar y coordinar proyectos de investigación para el desarrollo de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo de la sociedad mexicana.

- Promover el desarrollo de acciones encaminadas a la formación de recursos humanos capacitados en el uso de aplicaciones educativas y de tecnología avanzada de redes de telecomunicaciones y cómputo. "[1]

3.2 Historia de la Red de Datos de la DEPFI

La División de Estudios de Posgrado de la Facultad de Ingeniería (DEPFI) de la Universidad Nacional Autónoma de México (UNAM) es la institución pionera en educación de posgrados en ingeniería en América Latina, y junto con el Instituto de Ingeniería de la UNAM, se ha abocado a la investigación y desarrollo tecnológico, a la formación de personal docente de la más alta calidad, a la capacitación de personal de varias dependencias gubernamentales y organizaciones privadas, así como a la formación de profesionales que se han destacado en todos bs ámbitos del sector productivo del país. Su evolución siempre ha respondido a los cambios y necesidades del país logrando la vanguardia y reconocimiento de sus estudios en el nivel nacional e internacional.

La División de Estudios de Posgrado se establece el 23 de abril de 1957 con el nombre de División de Estudios Superiores (DESFI) al ser aprobado el proyecto de Reglamento y el Plan de Estudios por el H.

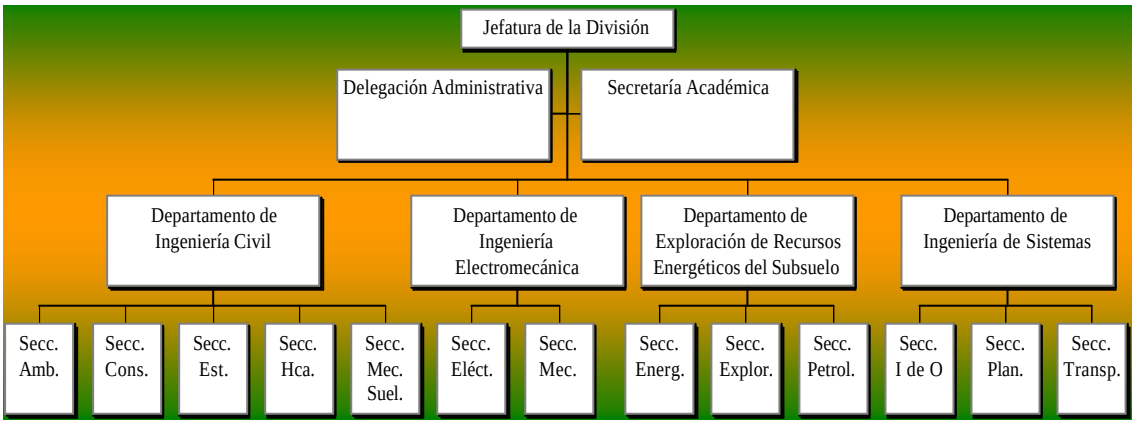
[1] www.dtd.unam.mx/internet.html

Consejo Técnico. A raíz de esta aprobación, el entonces Director de la Escuela Nacional de Ingeniería, Ing. Javier Barros Sierra, modificó la organización de la escuela, convirtió el Instituto de Ingeniería, A.C. en la División de Investigación, creó la División de Estudios Superiores y agrupó el resto de la escuela en la Escuela Nacional de Ingeniería. Así, ésta se convirtió en Facultad de Ingeniería. El cambio oficial fue aprobado junto con el Reglamento para la División del Doctorado por el Consejo Universitario hasta el 6 de agosto de 1959, cuando ya era director el Ing. Antonio Dovalí Jaime, y ocupaba todavía la rectoría, en un segundo período, el Dr. Nabor Carrillo Flores. Cuando esto sucedió, ya la DEPFI ocupaba un edificio propio, de tres plantas con aproximadamente 762 m2 dedicados a oficinas, aulas, biblioteca y laboratorios.

El objetivo de la DEPFI es:

"Satisfacer las necesidades de la educación superior a la Licenciatura, en diversas ramas de la Ingeniería, para formar profesionales especializados, profesores e investigadores"

La DEPFI se encuentra organizada de acuerdo en el siguiente organigrama:



Actualmente la DEPFI administrativamente desapareció, convirtiéndose en la Secretaría de Posgrado e Investigación. Sin embargo, para la realización del presente trabajo, no hubo ningún cambio.

Red de la Facultad de Ingeniería

En 1989 la Facultad de Ingeniería se incorporó a la REDUNAM y por medio de ésta se accedió a Internet. Inicialmente se asignaron a la Facultad tres dominios de trabajo, los cuales fueron:

- depfi.unam.mx, empleado por la División de Posgrado en algunas áreas de los Edificios A y B.
- fidieec.unam.mx, asignado a la antigua División de Ingeniería Eléctrica, Electrónica y en Computación, actualmente la División de Ingeniería Eléctrica (DIE).
- cecafi.unam.mx, utilizado por el antiguo Centro de Cálculo de la Facultad de Ingeniería.

La Red de Datos de la Facultad de Ingeniería fue una de las primeras en anexarse a la REDUNAM en Ciudad Universitaria. Su construcción data de finales de la década de los 80. Posteriormente la DEPFI se conecto a la red de la FI, así como a la REDUNAM.

En 1995, a través del proyecto "Red de la Facultad de Ingeniería" se inició de manera planeada la implantación de la red de cómputo de la Facultad de Ingeniería, con lo cual se logró comunicar los diecinueve edificios que conforman la Facultad. La red implantada fue una red Ethernet que cumple con el estándar IEEE 802.3 a 10 Mbps, con un backbone de fibra óptica multimodo (62.5/125 μm) y conexión a través de Hubs. Los equipos principales fueron Hubs para fibra óptica con conexión ST. El cableado fue semiestructurado.

Para llevar a cabo la implantación de la red, fue necesaria la participación de todas las áreas de la Facultad a través de sus representantes, y la colaboración de la DGSCA y de la Dirección General de Obras (DGO).

Con este proyecto se agregaron dos dominios a los ya existentes, por lo que fue necesario uniformizar las nomenclaturas de éstos y, para propósitos administrativos, se dividió la FI en cuatro zonas, quedando de la siguiente manera:

Zona	*Nombre del Dominio*	*Rango de Direcciones IP*	*Gateway*	*Ubicación*
P	fi-p.unam.mx	132.248.52.0/24	132.248.52.254	Edificios de posgrado
A	fi-a.unam.mx	132.248.54. 0/24	132.248.54.254	Edificio principal
B	fi-b.unam.mx	132.248.59. 0/24	132.248.59.254	DIMEI y Valdés Vallejo
D	mineria.unam.mx	132.248.138. 0/24	132.248.138.254	Palacio de Minería.
C	fi-c.unam.mx	132.248.139. 0/24	132.248.139.254	DICTyG, Anexo, Talleres de Mecánica, Lab. de Termofluidos, Biblioteca, UNICA y DCB.

Tabla 3.1 Dominios asignados a la FI

Los servidores de nombre (DNS) utilizados fueron: ns.dgsca.unam.mx (132.248.10.2), noc.noc.unam.mx (132.248.204.1), (132.248.237.250) y danzon.astroscu.unam.mx (132.248.1.3).

Como se puede observar en la Figura 3.2 las zonas A, B y C, son compartidas por varias divisiones, por lo que fue necesario realizar subredes internas a ellas, asignándoles un rango de direcciones IP a cada área que las necesitara.

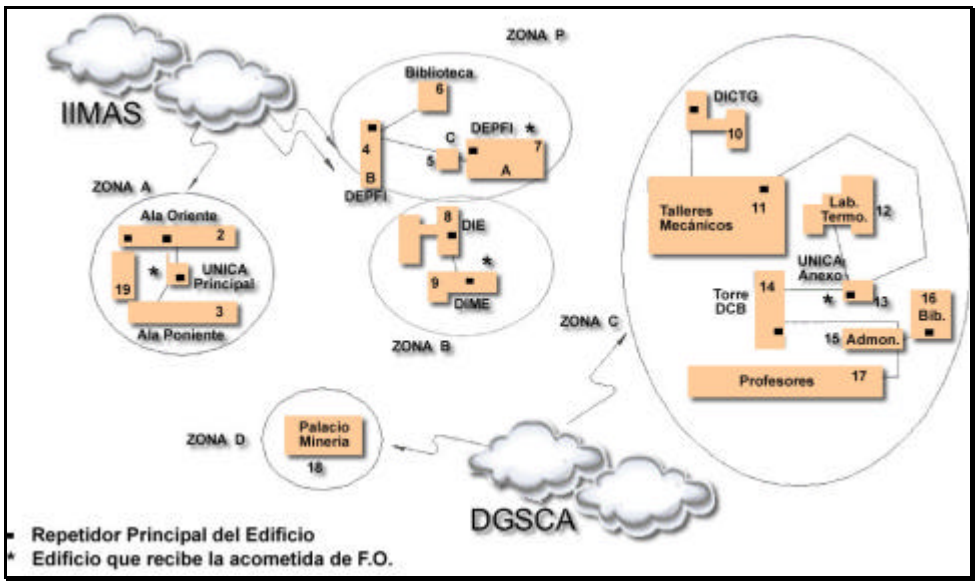


Figura 3.2 Conexión de edificios de la Facultad de Ingeniería a REDUNAM

Red de la DEPFI

La División de Estudios de Posgrado, hasta 1998 estaba compuesta por cuatro Edificios, nombrados A, B, C y Biblioteca (ver Figura 3.3). En los Edificios A y B se encontraba instalada la red LAN de la División, con un backbone de cable coaxial a una velocidad de 10 Mbps. La conexión a REDUNAM se realizaba a través del IIMAS con un enlace de fibra óptica multimodo (62.5/125 μm), la cual llegaba al segundo piso del Edificio A.

El cableado en las zonas de trabajo no era estructurado y estaba basado en cable UTP categoría 3. El edifico B sólo tenía zonas de trabajo en el ala oriente, por lo que solamente ahí había red. La conexión entre el ala oriente del Edificio B y la Biblioteca se realizaba con fibra óptica multimodo (62.5/125 μm). El edificio C no contaba con servicios de red.

Los dispositivos que se emplearon para brindar el servicio de red a los usuarios finales eran Hubs a 10 Mbps.

Para 1995, la División tenía los siguientes requerimientos[2]:

- "Conexión a REDUNAM por medio de fibra óptica al Edificio "C" de la DEPFI, ya que se encontraba aislado y su ubicación era de sumo interés académico, de investigación y administrativas

- "Cambio del backbone de los Edificios A y B de cable coaxial grueso a fibra óptica. Había la posibilidad de hacerlo por medio de concentradores de fibra óptica. Esta opción fue

[2] Documento proporcionado por el Laboratorio de Cómputo del Departamento de Sistemas, DEPFI, UNAM.

considerada pensando en el futuro crecimiento de la red en ambos Edificios, así como mejorar la transmisión.

- "Hubs de 12 puertos para el Edificio A ya previo al estudio realizado en ese momento se habían instalado recientemente y no contaban con el servicio de REDUNAM. El segmento conectado al cable coaxial sufría caídas debido a la saturación de equipos conectados a éste.

- "Se requería de un Hub para la planta baja del Edificio B, el cual daría un servicio a toda el área administrativa de este Edificio, en donde se encuentran las áreas de contabilidad, servicios escolares y personal académico.

- "Así mismo, para el primer piso del Edificio B se requería de un Hub, ya que no se contaba con acceso a REDUNAM en la sección del Departamento de Hidráulica.

- "Como parte complementaria, se decidió acondicionar el auditorio para contar con servicios de Teleconferencia, ya que se consideró de primordial interés para la docencia, y la actualización profesional que se llevan a cabo en el Posgrado."

Cabe mencionar que estos requerimientos no fueron cubiertos en su totalidad en aquel tiempo.

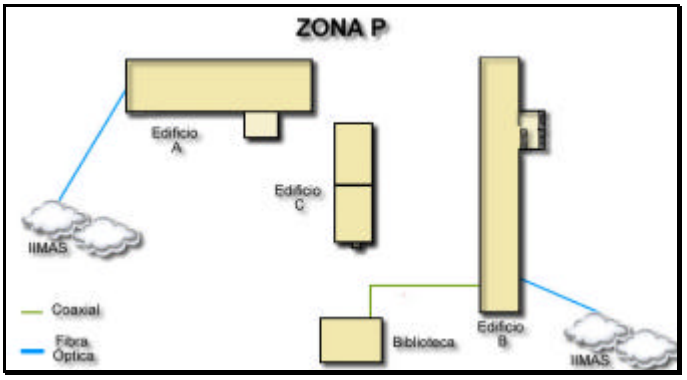


Figura 3.3 Conexión de Edificios de la DEPFI a REDUNAM antes de 1998.

La última actualización a la Red de Datos de la DEPFI (Ver Figura 3.4) se llevó a cabo tras la inauguración del Edificio Bernardo Quintana en agosto de 1998. Ésta consistió en un nuevo backbone de fibra óptica multimodo (62.5/125 μm) el cual sólo se cableó y a la fecha no se encuentra en operación. El backbone funcional está construido con cable UTP categoría 5. Los equipos principales fueron Hubs para fibra óptica con conexión SC, los cuales se encuentran en cada piso y distribuyen la conexión de la red hacia los usuarios finales. El cableado fue semiestructurado con cable UTP Categoría 5.

La DEPFI no cuenta con memorias técnicas o cualquier otro documento que muestre el desarrollo del proyecto de modernización realizado.

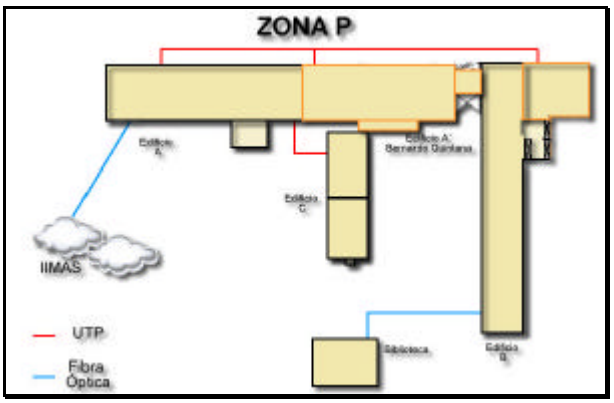


Figura 3.4 Interconexión actual de los Edificios de la DEPFI y la REDUNAM

3.3 Políticas de Red de la Facultad de Ingeniería

Introducción

Conforme a transcurrido el tiempo a partir de la segunda década de los '80, los incidentes de seguridad, comenzaron a acaparar la atención de propios y extraños, los medios masivos de comunicación descubrieron una nueva mina de oro al dar a conocer al público los detalles, una infinidad de ataques de los cuales una mayoría son publicados por Agencias de Seguridad computacional a través de Internet, y otras tantas, ni siquiera son detectados.

La Seguridad en Cómputo va mucho más allá de impedir que los "chicos malos" se roben la información y puedan hacer mal uso de ella. También implica proteger a los usuarios contra sus propios errores, o sugerir a los administradores realizar a tiempo sus respaldos. Los problemas cotidianos son mucho menos "atractivos" que la persecución de un espía alemán a través de redes de cómputo, pero son igual de importantes, de manera que es necesario estar preparados para hacerles frente.

La Facultad de Ingeniería (FI), como cualquier otra dependencia o institución es un posible blanco de ataques informáticos que pueden poner en peligro la integridad de los recursos informáticos, ya sean dispositivos de cómputo como información. Por tal motivo se elaboró un documento en el que se dan a conocer las medidas a tomar para reducir la posibilidad de ser atacados, tanto por gente interna como por externa a la FI.

El documento de POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA LA FACULTAD DE INGENIERÍA (Ver Anexo A) fue realizado por el SUBCOMITÉ DE ADMINISTRADORES DE RED de la misma Facultad. En ella se plasman una serie de lineamientos a los cuales deberán apegarse todas aquellas áreas en las que se haga uso de recursos de cómputo dentro de la institución.

En éste documento se establece "un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella y lo que no está, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a éstos."[3] Para tal efecto se establecen políticas y procedimientos.

Con esta serie de lineamientos, se pretende crear una cultura en el uso óptimo y correcto de los recursos informáticos de la FI. De tal forma que el apegarse a dichos lineamientos "conllevará a hacer de la red de cómputo de la Facultad y el Internet un ambiente más seguro y productivo para estudiantes y miembros en general de la comunidad universitaria"[4].

Hacer un uso de los lineamientos beneficia a:

- Administradores: se reducen riesgos en el manejo de la infraestructura y la información. Le permite actuar en forma y tiempo ante alguna contingencia informática.
- Usuarios: uso óptimo y correcto de los recursos informáticos. Seguridad en la información. Disponibilidad de los recursos.

A continuación se resumen los puntos que trata éste documento así como también se describen mas acciones que la DEPFI lleva a cabo para el seguimiento de las Políticas de Seguridad en Cómputo.

Seguridad en Cómputo

Se refiere a las características de los recursos informáticos, tanto físicos como lógicos, que permiten a los usuarios de la institución hacer uso correcto de dichos recursos (hardware e información). Se establece que toda información debe ser confidencial, integra, disponible, mientras que para los recursos físicos, éstos deben ser consistentes y se requiere una autentificación mediante un control de acceso.

Para lograr lo anterior se sugiere una constante capacitación hacia lo usuarios para que puedan conocer el uso adecuado de los sistemas de computo y saber actuar ante cualquier anomalía. Esto en la DEPFI no se lleva a cabo de forma institucional al no existir un Administrador de red que promueva la importancia y la cultura de seguridad informática.

Políticas de Seguridad Física

En esta sección se describen las medidas de seguridad que se requieren para proteger todas aquellas instalaciones en las que se cuente con sistemas de computo, tanto para equipo critico como de usuario final.

[3] Políticas de Seguridad en Cómputo para la Facultad de Ingeniería, marzo de 2003
[4] Idem.

En este punto, por parte de la DEPFI, no se cumplen con algunos de los lineamientos de este documento. Tal es el caso de la falta de extintores en salas de computo, instalación de NO-BREAKS en equipos críticos y el consumo de alimentos en lugares donde se encuentran equipos de computo.

Políticas de Cuentas

Se establecen los requisitos para poder asignar una cuenta de usuario, el cómo esta conformada y quien tiene esta autorizado para asignarla. Estas cuentas deben asignadas por el Encargado o el Administrador de red de área local únicamente al personal autorizado y legitimo (miembros vigentes de la FI y personal autorizado en proyectos especiales) de tal forma que estas cuentas sean personales e intransferibles.

Estas prácticas dentro de la DEPFI si son llevadas a cabo por cada encargado de sección.

Políticas de Contraseñas

Las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Se establece quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada. Como en el punto anterior el Encargado o el Administrador de red de área local es la persona autorizada para la asignación de contraseñas.

Cada sección tiene servicios propios para sus usuarios por lo que la asignación de contraseñas se lleva a cabo mediante la solicitud del usuario. Estas contraseñas no se apegan a un formato en especial salvo las requeridas por la aplicación. En computadoras personales, el usuario final es quien establece su contraseña en forma individual con total desconocimiento de las políticas correspondientes.

Políticas de Control de Acceso

En este apartado de especifican cómo, desde dónde y de qué manera los usuarios deben autentificarse. Aquí se establecen los procedimientos y requerimientos necesarios para que un usuario pueda realizar conexiones remotas y salvaguardar la integridad de los equipos y la información.

En la DEPFI se llevan a cabo sesiones de conexión remota que son empleadas para compartir recursos, información, etc. necesarias para la investigación y la docencia. Sin embargo no se tiene un control estricto debido al desconocimiento de las políticas correspondientes.

Políticas de Uso Adecuado

Se describe lo que se considera como "Uso Adecuado" o "Inadecuado" de los sistema informáticos por parte de los usuarios. De igual forma se indica lo que "Está Permitido" y lo que "Está Prohibido". Para ello se clasifica lo que es permisivo o lo prohibitivo en el uso de recursos informáticos.

Este es un gran problema. Ya que no se cuenta con un Administrador de la Red de Datos de la DEPFI no es posible identificar a los usuarios que hacen uso de software que están catalogados en las Políticas como Prohibidos. El problema que aquí se presenta es que debido a la gran cantidad de computadoras que hacen uso de aplicaciones para compartir archivos (kazaa, napster, etc.) el trafico en la red es alto y ocasiona la reducción del ancho de banda en la red.

En la actualidad se pueden descargar de la Internet una gran cantidad de aplicaciones que pueden afectar la seguridad de los equipos y la información y no se tiene un control sobre estas actividades.

Políticas de Respaldos

Se refiere a la responsabilidad, tanto por parte del usuario como del administrador para realizar los respaldos necesarios de la información.

El usuario final es responsable de la información generada por el mismo. Esto generalmente no se lleva a cabo debido a un total desconocimiento de éstas políticas así como la falta de una cultura informática. Es importante llevar a cabo las medidas necesarias para salvaguardar la información en los equipos debido a la que la Red de Datos de la DEPFI es muy vulnerable a ataques informáticos.

Políticas de Correo Electrónico

En este apartado se establece el uso adecuado y no inadecuado del servicio de correo electrónico, así como los derechos y obligaciones a los que están sujetos los usuarios que hacen uso de este servicio.

En este sentido no se tiene un control del uso del correo electrónico debido a que no se realizan monitoreos para determinar un uso inadecuado.

La DGSCA realiza la notificación en el momento en el que se un servidor o una cuenta de correo electrónico esta generando SPAM o retransmitiendo un virus. En este momento se toman las medidas necesarias (aplicar los parches para eliminar el virus o desconectar el servidor) para evitar la suspensión del servicio de por parte de la DGSCA.

Políticas de Contabilidad del Sistema

Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que debe manejarse la contabilidad del sistema y el propósito de la misma.

En la DEPFI no se tiene control de este punto. En la Internet es posible encontrar aplicaciones que se pueden descargar que realizan funciones de monitoreo en la red. Estas aplicaciones deben ser controladas debido a que están prohibidas (como se menciona en las Políticas) y pueden afectar la seguridad de los equipos y la información. Únicamente el Administrador de la Red de Datos de la DEPFI y el personal autorizado puede hacer uso de estas aplicaciones con fines estadísticos y de control.

Políticas de Uso de Direcciones IP

Las políticas de Seguridad en Cómputo para la Facultad de Ingeniería establecen el uso adecuado y las consideraciones con respecto al uso y asignación de direcciones IP.

A pesar de que en la DEPFI se cuenta con un registro (inventario) de las direcciones IP asignadas a cada una de las secciones, no se puede considerar como una información confiable. Esto se debe a que se han presentado casos en los que los usuarios realizan cambios en la configuración de los equipos o hacen uso de aplicaciones DHCP (configura la primer dirección IP disponible) y esto provoca que el usuario propietario de la dirección IP quede inactivo.

No se lleva a cabo el aviso correspondiente de los cambios en la direcciones IP ni en el cambio de tarjetas de red (necesario para la dirección MAC de la tarjeta).

Aunque están permitido el uso de rangos de direcciones privadas 192.168.0.0/16, no se tiene un control de la asignación de éstas.

Políticas de Contratación y Finalización de Relaciones Laborales de Recursos Humanos en Sistemas Informáticos

En este apartado se sugieren los procedimientos que se deben llevar a cabo para el personal cuando se les asigna la responsabilidad del uso de sistemas informáticos críticos, así como cuando finaliza esta responsabilidad.

A ciencia cierta se desconocen los procedimientos que se llevan en este sentido, ya que cada sección es responsable de la asignación del personal, aunque se puede suponer que se llevan a cabo estas medidas por la seguridad propia de los recursos y la información.

Sanciones

En esta sección se detallan una serie de causas y el qué hacer en caso de violaciones en los sistemas informáticos y así como de estas políticas. Se dan a conocer una serie de incidentes que pueden poner en riesgo la seguridad de los sistemas informáticos y que son motivo de sanciones. Las sanciones están dadas por la suspensión del servicio desde un día hasta un año; la cancelación del servicio durante su estadía en la carrera; cartas de extrañamiento.

Debido a la falta de un Administrador de Red en la DEPFI y de los medios para hacer del conocimiento la existencia de estas políticas no es posible aplicar las sanciones que se establecen en este documento, a pesar de que continuamente se llevan a cabo violaciones a los sistemas informáticos y se tiene constantes incidentes de seguridad en los mismos.

Plan de Contingencias

Se definen los "procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles"[5].

En la DEPFI no se cuentan con dichos planes ni con el personal encargado en atender alguna emergencia en equipos de cómputo e información. Cada sección de la División da solución a corregir los problemas de seguridad interna con su propio personal.

3.4 Sumario del Estado Actual de la Red de Datos de la DEPFI

Actualmente la red de datos de la DEPFI está basada en una tecnología Ethernet a 10 Mbps, con una topología de árbol y un cableado semiestructurado, así como un backbone de cable UTP categoría 5.

La llegada de la señal de REDUNAM a la red de datos de la DEPFI se encuentra ubicada en el Área de la Sección de Ingeniería Eléctrica, en el segundo piso del Edificio A de ésta División. Se trata de un par de fibra óptica multimodo (62.5/125 μm) con conectores ST; el ancho de banda asignado a este segmento de red es de 10 Mbps, el cual es proporcionado por un LANplex 2500, ubicado en el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS). El LANplex está identificado dentro del IIMAS como LANplex IIMAS-DGAE bajo la IP 132.248.255.72.

La señal es recibida en un transceiver de fibra óptica – AUI, conectado a un switch 10/100 Mbps 3Com, el cual distribuye la señal.

[5] Políticas de Seguridad en Cómputo para la Facultad de Ingeniería, marzo de 2003

La distribución de la señal del switch de la llegada principal se realiza conectando en cascada varios Hubs, de los cuales se distribuye hacia las áreas de los usuarios. Los puertos del switch, a excepción de uno, alimentan exclusivamente a los Hubs y estaciones de trabajo (pc's, ws, servidores, impresoras, etc.) del segundo piso de los Edificios A y Bernardo Quintana.

Un solo puerto del switch alimenta a los Hubs en cascada de la planta baja, primero y tercer piso de los Edificios A y Bernardo Quintana, así como del Edificio B y de la Biblioteca.

Cabe señalar que este Hub lleva toda la carga del tráfico de las áreas anteriormente descritas. Por otro lado, la conexión entre el Edificio B (ala oriente) y la Biblioteca se realiza mediante fibra óptica multimodo (62.5/125 µm) (Ver Figura 3.5).

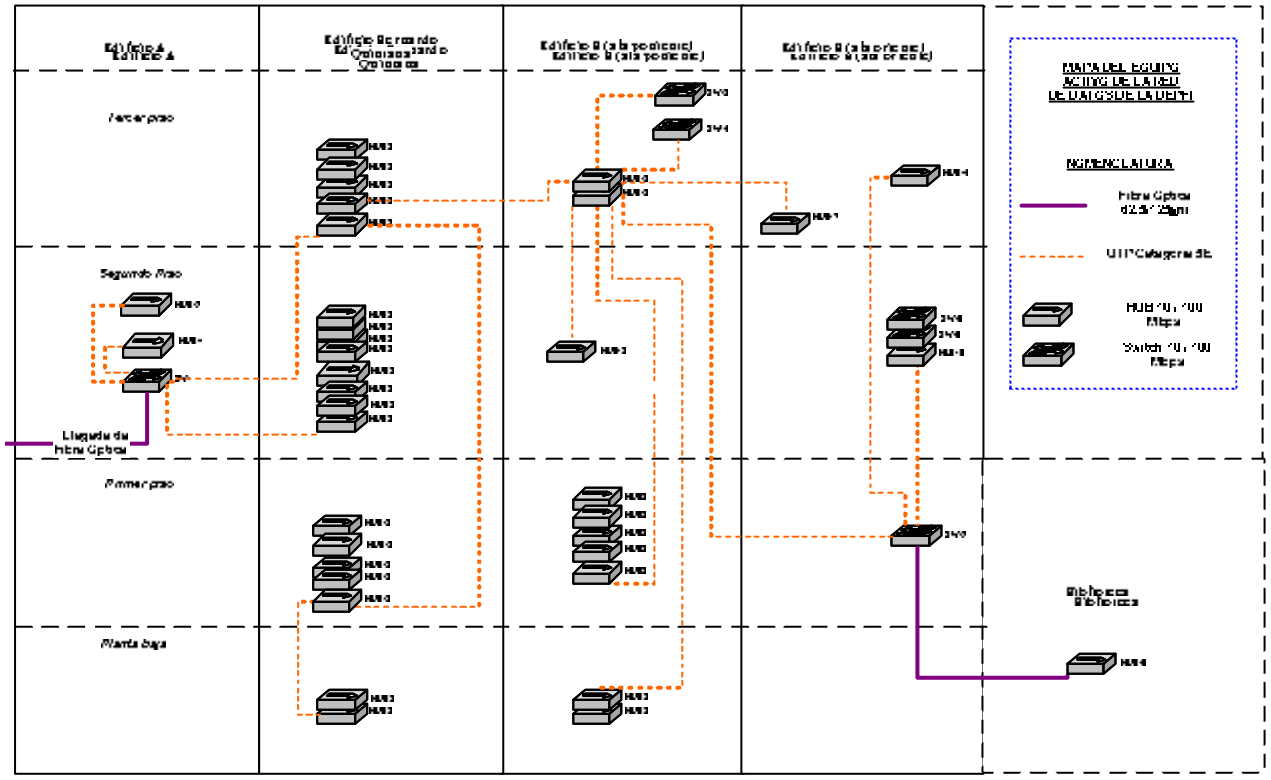


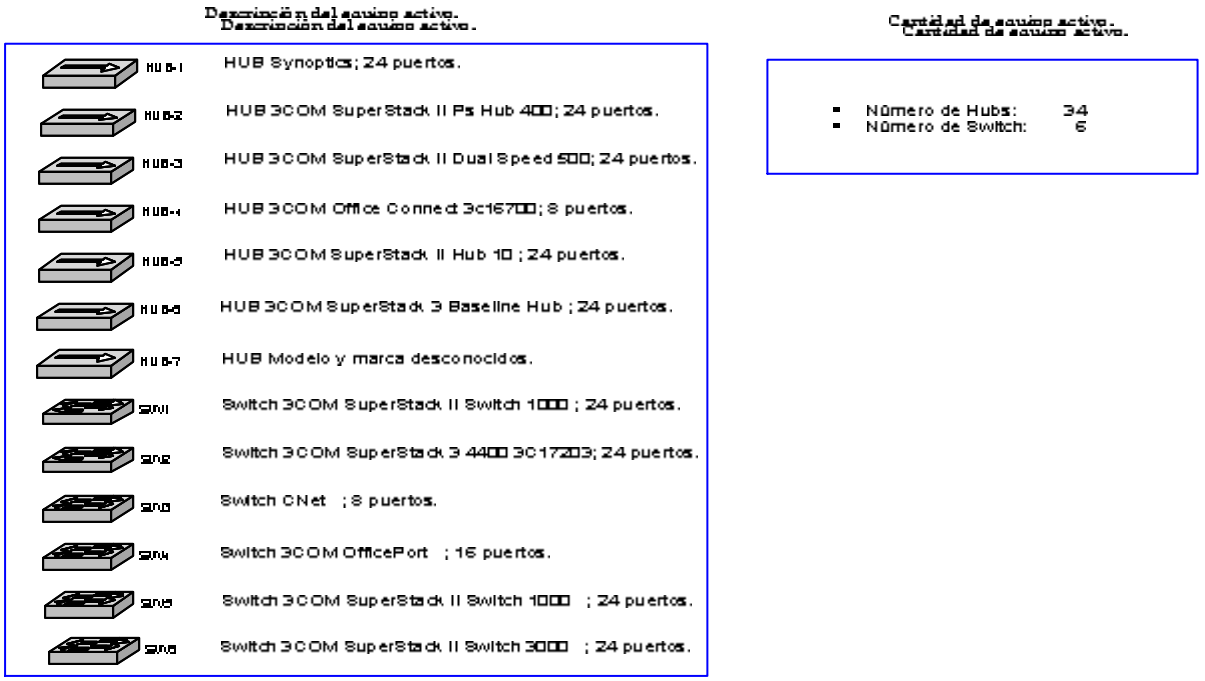
Figura 3.5 Equipo activo de la red de datos de la DEPFI.

La cantidad de equipos que actualmente están siendo utilizados, distribuidos por área y nivel, son los siguientes:

NIVEL	ÁREA	Hubs	Switch
Planta Baja	EDIFICIO "A"	0	0
Primer Piso		0	0
Segundo Piso		2	1
Tercer Piso		0	0
Planta Baja	EDIFICIO "BERNARDO QUINTANA"	2	0
Primer Piso		5	0
Segundo Piso		8	0
Tercer Piso		5	0
Planta Baja	EDIFICIO "B" (ala poniente)	2	0
Primer Piso		5	0
Segundo Piso		1	0
Tercer Piso		2	2
Planta Baja	EDIFICIO "B" (ala oriente)	0	0
Primer Piso		0	1
Segundo Piso		1	2
Tercer Piso		2	0
Planta Baja	Biblioteca	0	0
Primer Piso		1	0
	TOTAL DE EQUIPOS:	36	6

Tabla 3.1 Equipo activo

Los modelos, las marcas y la simbología utilizada en la Figura 3.5, de los equipos activos se muestran en la Figura 3.6.



CAPÍTULO 4

ANÁLISIS DEL ESTADO ACTUAL DE LA RED DE DATOS DE LA DEPFI.

Este capítulo tiene el propósito de dar un diagnóstico a las condiciones en las que se encuentra la red de datos de la DEPFI, tomando en cuenta su infraestructura tecnológica y administrativa.

Se describe la topología física de la red, tomando en cuenta sus medios de transmisión, los equipos activos y la distribución de la red a través de los edificios de la DEPFI. Posteriormente, se menciona el estándar que permite hacer uso de direcciones IP reservadas, como antecedente a la descripción de la topología lógica de la red de la DEPFI.

Además, se describen las herramientas de software utilizadas para llevar a cabo las mediciones necesarias que permitieron conocer el nivel de utilización de la red, así como diagnosticar problemas y tendencias de comportamiento. Se proporcionan diferentes muestras de mediciones realizadas durante el desarrollo de este trabajo, que muestran situaciones de bajo desempeño en la red.

Por último, se mencionan la situación en la que se encuentra el cableado estructurado de la red, así como la situación administrativa.

4.1 Topología Física de la Red

Actualmente la DEPFI cuenta con cinco edificios. Los usuarios finales que se encuentren en la DEPFI pertenecen a diferentes áreas de los posgrados que imparte esta Facultad. Debido a su heterogeneidad, las necesidades de comunicación de datos son diferentes. Sin embargo, podemos encontrar un número de servicios estándar que son proporcionados a través de la Red de Datos, entre los cuales se encuentran servidores de correo electrónico, de páginas Web y de transferencia de archivos. Para proporcionar esos servicios y otros a aplicaciones específicas de las distintas áreas de ingeniería que aquí se desarrollan, el funcionamiento de la Red de Datos debe ser el óptimo.

Como se mencionó en el capítulo anterior, la llegada de la señal de REDUNAM a la Red de Datos de la DEPFI se encuentra ubicada en el Área de la Sección de Ingeniería Eléctrica, en el segundo piso del Edificio A de esta División. Se trata de un par de fibra óptica multimodo (62.5/125 μm) con conectores ST; el ancho de banda asignado a este segmento de red es de 10 Mbps. La señal es recibida en un transceiver de fibra óptica – AUI.

El backbone activo de esta red está basado en cable UTP categoría 5. Este backbone se distribuye a lo largo de los edificios A, B y Bernardo Quintana. La conexión entre el Edificio B (ala oriente) y la Biblioteca está basada en fibra óptica multimodo (62.5/125 μm) (Ver Figura 4.1)

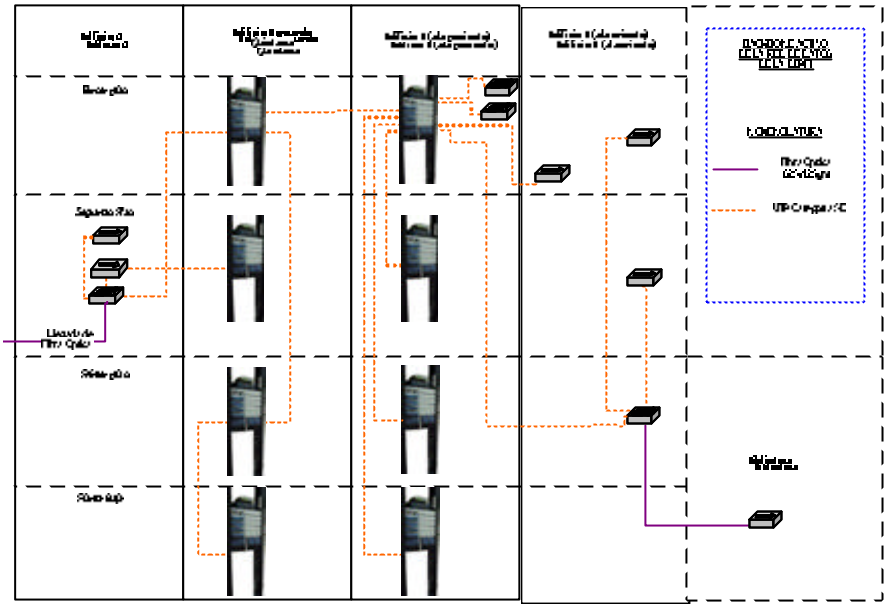


Figura 4.1 Backbone Activo de la Red de Datos de la DEPFI

En los Edificios A, B (ala poniente) y Bernardo Quintana se encuentra cableado un backbone de fibra óptica multimodo (62.5/125 µm) (Ver Figura 4.2), el cual no se encuentra habilitado. Cabe mencionar que algunos de los hilos de fibra óptica de este backbone no son funcionales, debido principalmente a que no se encuentran bien rematados o el conector no está bien sujeto al hilo.

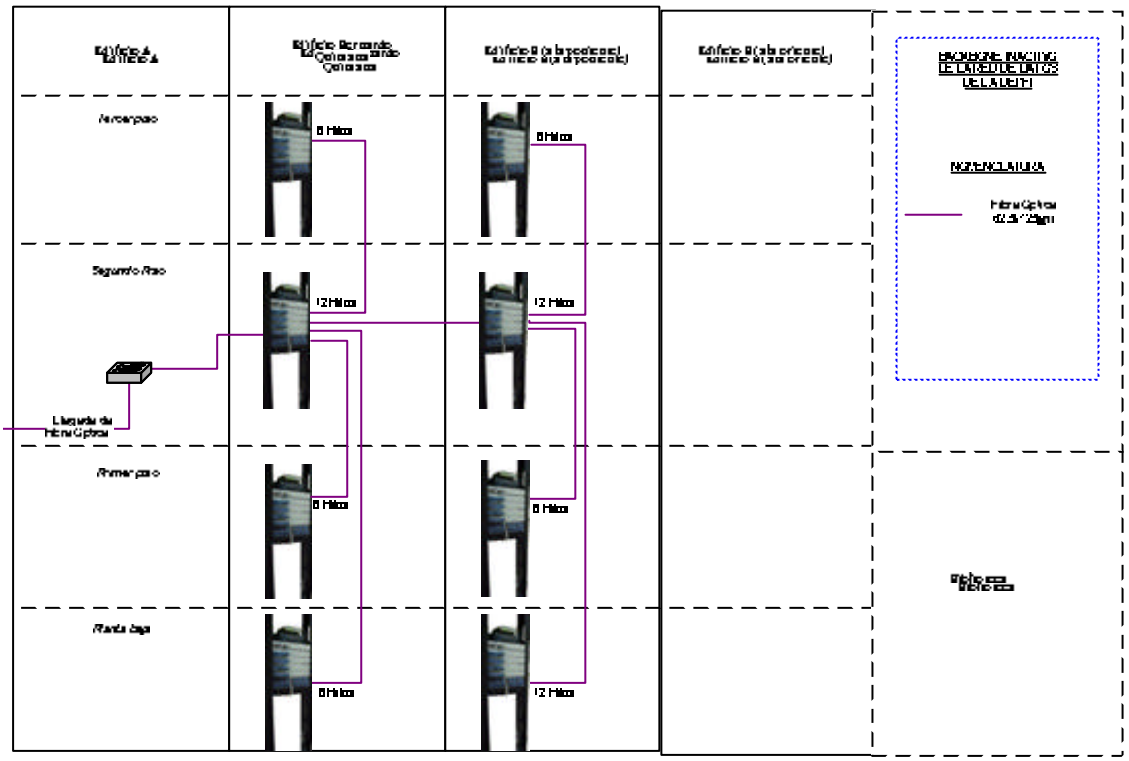


Figura 4.2 Backbone Inactivo de la Red de Datos de la DEPFI

Los equipos activos que actualmente son utilizados por la Red de Datos de la DEPFI son Switch's y Hubs. El switch principal es un 3COM SuperStack II 1000, que puede manejar anchos de banda de 10/100 Mbps y se encuentra en la llegada de fibra óptica proveniente del IIMAS. Conectados en cascada, se encuentran los Hubs y demás Switch's. La gran mayoría de los Hubs son del modelos SuperStack II Dual Speed 500 de 3COM, a 10/100 Mbps. Estos modelos permiten un nivel de apilamiento de hasta ocho hubs.

Se cuenta con un Core Builder 3500 de 3COM, el cual podría ser utilizado para activar el backbone de fibra óptica, sin embargo, hasta la fecha no ha sido conectado. Este modelo ya ha sido descontinuado por el fabricante, pero el equipo que se tiene aún es funcional. Cuenta con cuatro módulos, con capacidad de seis puertos SC 100BaseFX multimodo o monomodo cada uno.

La Figura 4.3 muestra la distribución y el número de equipos activos de la red. En ella se observa que el número de conexiones en cascada (saltos) de los Hubs que despachan las señales a todos los edificios supera por mucho las recomendaciones generales en el diseño de redes (cinco saltos), así como las recomendadas por los propios fabricantes. También se puede observar que se realizó una agrupación de los equipos, con el propósito de analizar el comportamiento de la carga de tráfico.

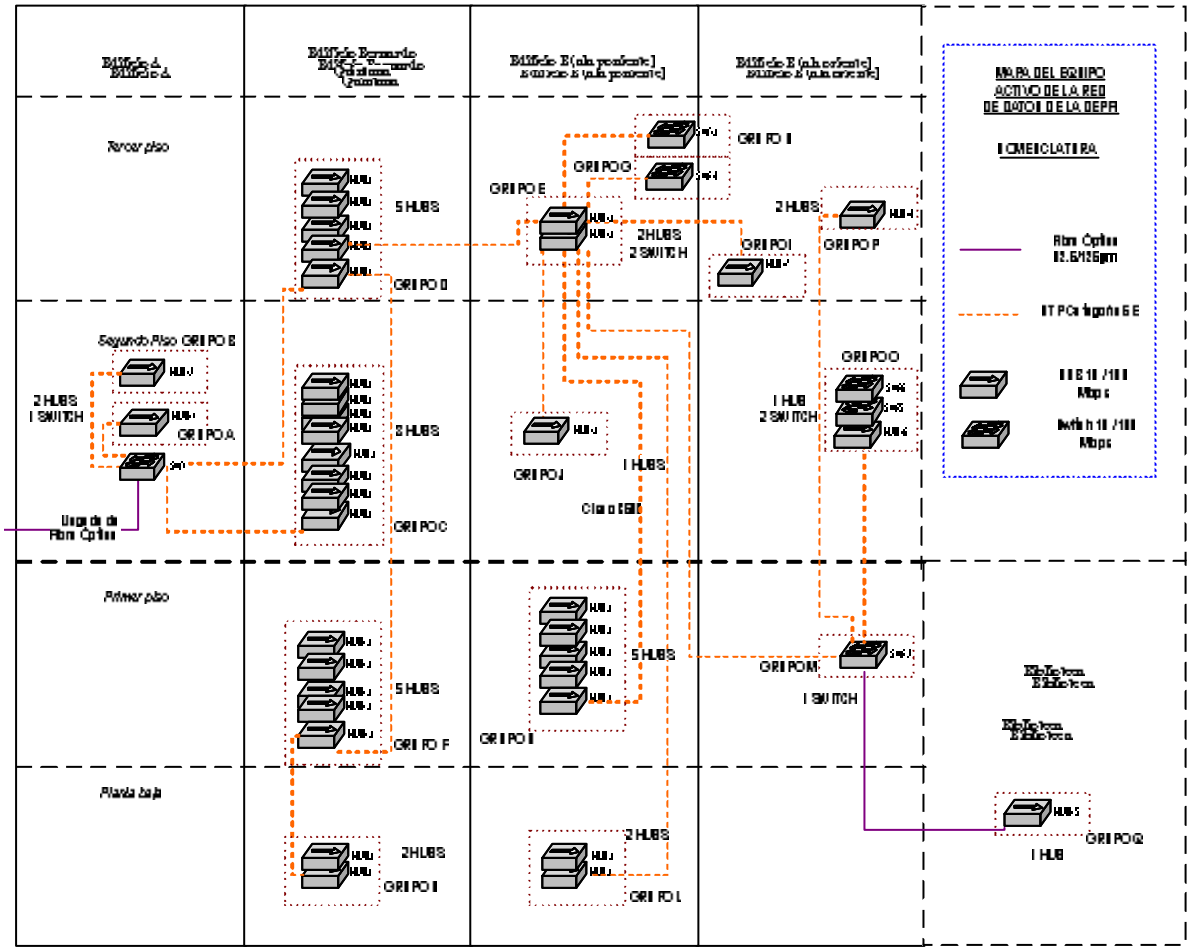


Figura 4.3 Mapa de Equipo Activo de la Red de Datos de la DEPFI - Grupos

El criterio empleado para la asignación de los grupos consistió principalmente en su ubicación física dentro de las instalaciones de la DEPFI, considerando los equipos que están conectados en cascada. En la siguiente tabla se identifica la localización de dichos grupos:

ÁREA	NIVEL	GRUPOS
EDIFICIO "A"	Planta Baja	-
	Primer Piso	-
	Segundo Piso	A, B
	Tercer Piso	-
EDIFICIO "BERNARDO QUINTANA"	Planta Baja	N
	Primer Piso	F
	Segundo Piso	C
	Tercer Piso	D
EDIFICIO "B" (ala poniente)	Planta Baja	L
	Primer Piso	K
	Segundo Piso	J
	Tercer Piso	E, G, H
EDIFICIO "B" (ala oriente)	Planta Baja	-
	Primer Piso	M
	Segundo Piso	O
	Tercer Piso	I, P
BIBLIOTECA	Planta Baja	Q

Tabla 4.1 Ubicación de los grupos de equipos activos

Como parte del análisis se realizó un diagrama de la topología de árbol (Ver Figura 4.4) para representar los grupos que se establecieron anteriormente. Este diagrama hace notar las deficiencias en el diseño, el balanceo de carga de los equipos y el desempeño con los que opera la Red de Datos de la DEPFI.

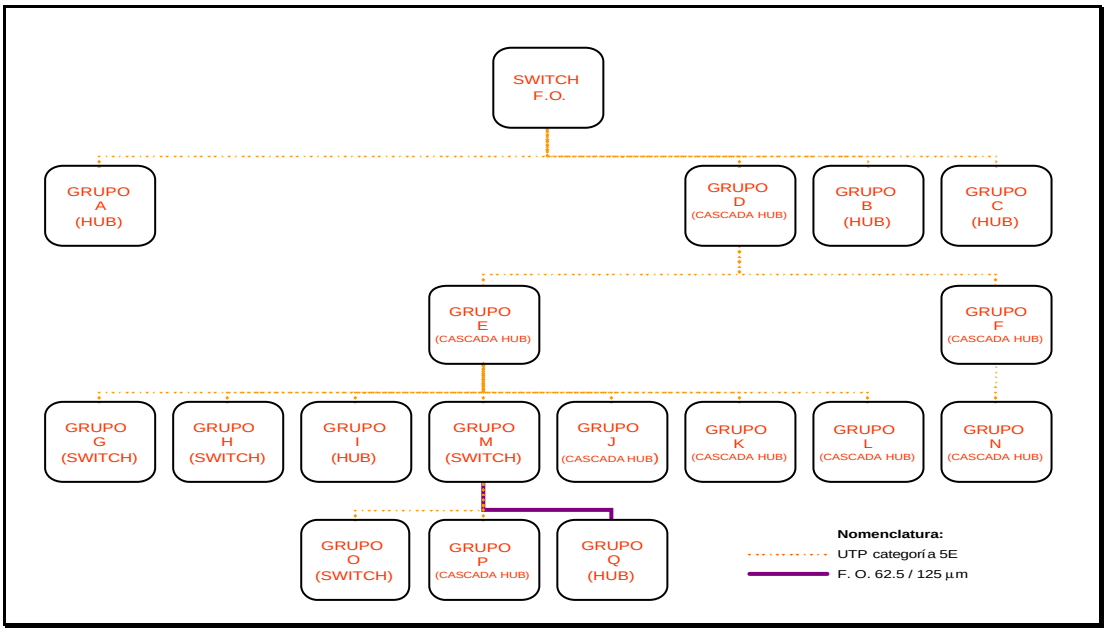


Figura 4.4 Topología de Árbol del Equipo Activo de la Red de Datos de la DEPFI

Como se puede observar en el diagrama de topología, al Grupo D (HUB 3COM SuperStack II Dual Speed 500 con 24 puertos) se encuentran conectados en cascada los Grupos E, F, G, H, I, J, M, K, L, N y los Grupos O, P y Q a través del Grupo M.

Los problemas que se presentan constantemente son el alto tráfico y el gran número de colisiones, que ocurren cuando las estaciones transmiten datos en la rama que se desprende del Grupo D, como consecuencia de la gran cantidad de equipos que de él dependen. Si el número de colisiones es excesivo se puede llegar a un estado de saturación de la red, que impide la comunicación. Cuando el tráfico se vuelve muy intenso el rendimiento de la red se degrada, provocando incluso, la caída de toda la red.

4.2 RFC 1918

La Petición de Comentarios (RFC)

Las series de documentos de Peticiones de Comentarios (RFC, por sus siglas en inglés) es un conjunto de notas técnicas y organizacionales acerca de la Internet, que comenzó en 1969. Los memos en las series RFC discuten varios aspectos de las redes de computadoras, incluyendo protocolos, procedimientos, programas y conceptos, así como notas de reuniones y opiniones.

Los documentos oficiales de especificaciones de la suite del Protocolo de Internet (IP) que son definidas por el Internet Engineering Task Force (IETF) y el Internet Engineering Steering Group (IESG) son grabadas y publicadas como "RFCs standards track". Como resultado, el proceso de publicación RFC juega un papel importante en el proceso de estándares de Internet.

Debido a la proliferación a nivel mundial de la tecnología TCP/IP, inclusive fuera de la Internet en sí, un número mayor de empresas no conectadas a ella usan esta tecnología y sus capacidades de direccionamiento para sus propias comunicaciones internas, sin ninguna intención de conectarse directamente a otras redes locales o a la misma Internet.

La práctica actual es asignar globalmente direcciones únicas a todos los host que hacen uso del protocolo TCP/IP. Existe una preocupación respecto del espacio finito de direcciones IP que podría quedar agotado.

Existen tres categorías en las que pueden clasificarse los host que usan IP:

- Host que no requieren acceso a host en otras redes locales o a lo largo de Internet.

- Host que necesitan acceso a un conjunto limitado de servicios externos (e.g. E-mail, FTP, netnews, acceso remoto) y que puede ser manejado por pasarelas (gateways) a nivel de aplicación.

- Host que necesitan acceso a nivel de red fuera de la red local, suministrado vía conectividad IP.

Los host dentro de la primera y segunda categoría pueden usar direcciones IP que son únicas dentro de la red local, pero que pueden ser ambiguas entre redes locales.

Solamente los host en la última categoría requieren direcciones IP que son únicas globalmente.

Existen muchas aplicaciones que requieren conectividad sólo dentro de una red local e incluso no necesitan conectividad externa para la mayoría de los host internos. En redes locales grandes, resulta fácil identificar un número sustancial de host usando TCP/IP que no necesitan conectividad a nivel de red, fuera de la propia red local.

La Autoridad de Asignación de Números de Internet (IANA) ha reservado los siguientes tres bloques del espacio de direcciones IP para redes privadas:

Segmento IP			*Bloque de bits*	*Clase de Red*
10.0.0.0	-	10.255.255. 255	24	A
172.16.0.0	-	172.31.255.255	20	B
192.168.0.0	-	192.168.255.255	16	C

Tabla 4.2 Espacio de direcciones privadas

El RFC 1918 permite, a quien desee hacer uso de las direcciones fuera del espacio de direcciones definido anteriormente (Ver Tabla 4.2), configurar una red sin la coordinación de la IANA o un registro de Internet, por lo que las direcciones en este espacio de direcciones privadas sólo serán únicas donde sean configuradas.

En ese documento se establece que para obtener un espacio de direccionamiento global se deberá hacer mediante un registro de Internet. Esto es, que las direcciones asignadas nunca corresponderán al bloque de direcciones IP definidas anteriormente.

Se definen como host privados a aquellos que no requieren tener una conectividad en la capa de red, fuera de la red local en un futuro cercano. Estos hacen uso del espacio de direcciones privadas definidas anteriormente, sin embargo, no podrán tener comunicación vía IP con cualquier host externo. Esto no interfiere con los servicios externos mediante la capa de aplicación.

El resto de los host son llamados públicos y hacen uso de un espacio de direccionamiento público asignado por un registro de Internet. Estos host pueden tener comunicación con otros host dentro de la misma red, sin importar si son públicos o privados, así como si son host públicos externos. Una característica es que los host públicos no tienen conectividad hacia host privados en otras redes locales.

Se considera que al realizar el cambio de un host privado a público (y viceversa) requiere de un cambio en la dirección IP.

Como las direcciones privadas no tienen un significado global, la información de enrutamiento sobre redes privadas no se propagará en enlaces entre alguna otra red, y los paquetes con dirección fuente o destino privados no serán remitidos a través de dicho enlace. Los ruteadores en las redes no hacen uso de espacio de direcciones privadas, especialmente de los Proveedores de Servicios de Internet (ISP), ya que se esperaría que estuvieran configurados para rechazar (filtrar) la información de enrutamiento sobre las redes privadas. Si uno de los ruteadores recibe información de rechazo, ésta no será tratada como un error en el protocolo de enrutamiento.

Las referencias indirectas de tales direcciones deberán estar contenidas dentro de la red local. Algunos ejemplos de dichas referencias son los Servidores de Nombre de Dominio (Domain Name Server) y otra información referida a las direcciones privadas internas. Los ISP deben tomar medidas para prevenir tales salidas.

La ventaja del uso del espacio de direcciones privadas para Internet es la conservación del espacio de direcciones único global, mediante el desuso de direcciones únicas donde no sean requeridas.

De igual forma, una red local goza de ventajas en cuanto al uso de direcciones privadas. Esto es, las redes locales ganan en la flexibilidad para el diseño, ya que se tiene más espacio de direccionamiento a su disposición. En otras palabras, se habilita la operatividad y los esquemas de administración de direcciones convenientes, así también, las facilidades de crecimiento.

Usar un espacio de direcciones privadas proporciona una elección segura para las redes locales, ya que se evitan choques una vez que la conectividad exterior sea necesaria.

En resumen, con el esquema descrito muchas organizaciones grandes sólo necesitarán un bloque relativamente pequeño de direcciones del espacio de direccionamiento global único. Los beneficios en Internet, con el tiempo, a través de la conservación del espacio de direcciones único global, prolongarán con eficacia la vida del espacio de direcciones IP. Las empresas se beneficiarán del incremento de flexibilidad suministrado por un espacio de direcciones relativamente grande.

4.3 Topología Lógica.

Debido a la limitante en el número de direcciones IP disponibles, las diferentes dependencias de la UNAM utilizan el esquema de direccionamiento sugerido en el RFC 1918, referente a la creación de espacios de direcciones privadas. En general, en la UNAM se crean espacios de direcciones de clase C, cuyo segmento es el 192.168.0.0/16.

La UNAM tiene asignado un bloque de direcciones IP de clase B (132.248.0.0/16), el cual es repartido entre las diferentes Entidades Universitarias que así lo requieran (Ver Figura 4.5). Por su parte, la DEPFI tiene asignado el segmento de red 132.248.52.0/24, el cual está distribuido entre las Secciones que componen esta División. Sin embargo, la utilización de las direcciones reales no es la misma entre los Departamentos. Mientras que algunos Departamentos no tienen los suficientes equipos para utilizar sus direcciones asignadas, hay otros que ya han sobrepasado en número, teniendo que recurrir a la utilización de Servidores de Traducción de Direcciones de Red (NAT, por sus siglas en inglés) para proporcionar la conectividad necesaria.

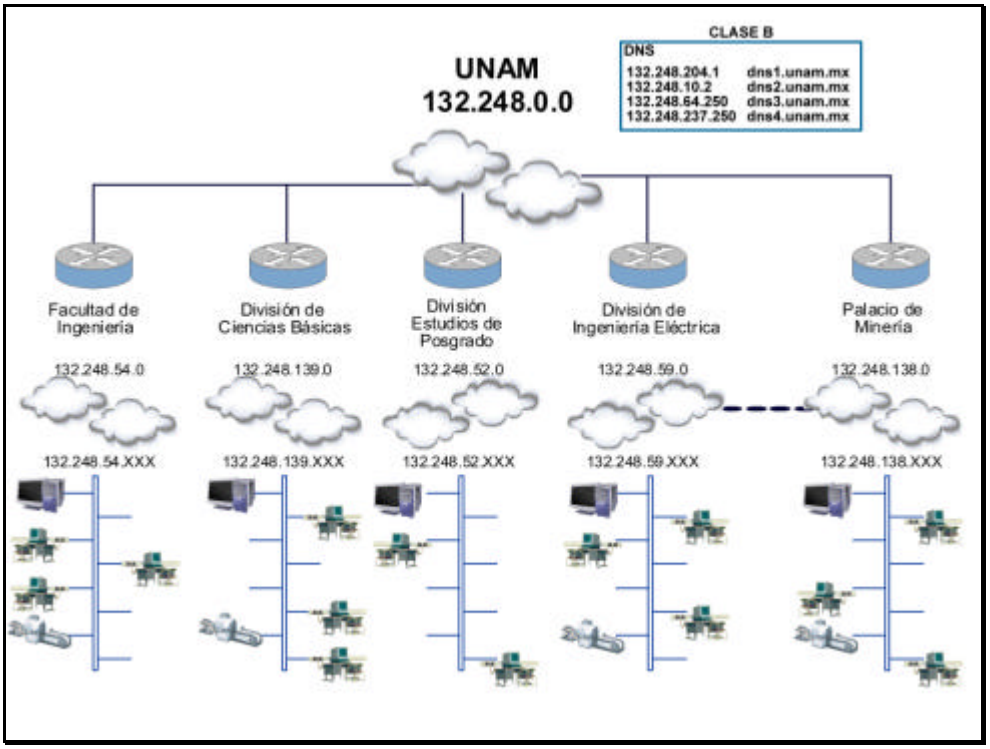


Figura 4.5 Topología lógica de la UNAM

Un ejemplo de ello es el Departamento de Sistemas, el cual además de hacer uso de las 26 direcciones reales asignadas, utiliza 15 direcciones de un segmento de direcciones reservadas (192.168.52.0/24), perteneciente a la Jefatura de la División y tiene su propio Servidor NAT con el segmento 192.168.0.0/24 disponible. Un inconveniente de los de servidores NAT es que aumentan el retraso de los paquetes, y por tanto, degradan el desempeño de la Red.

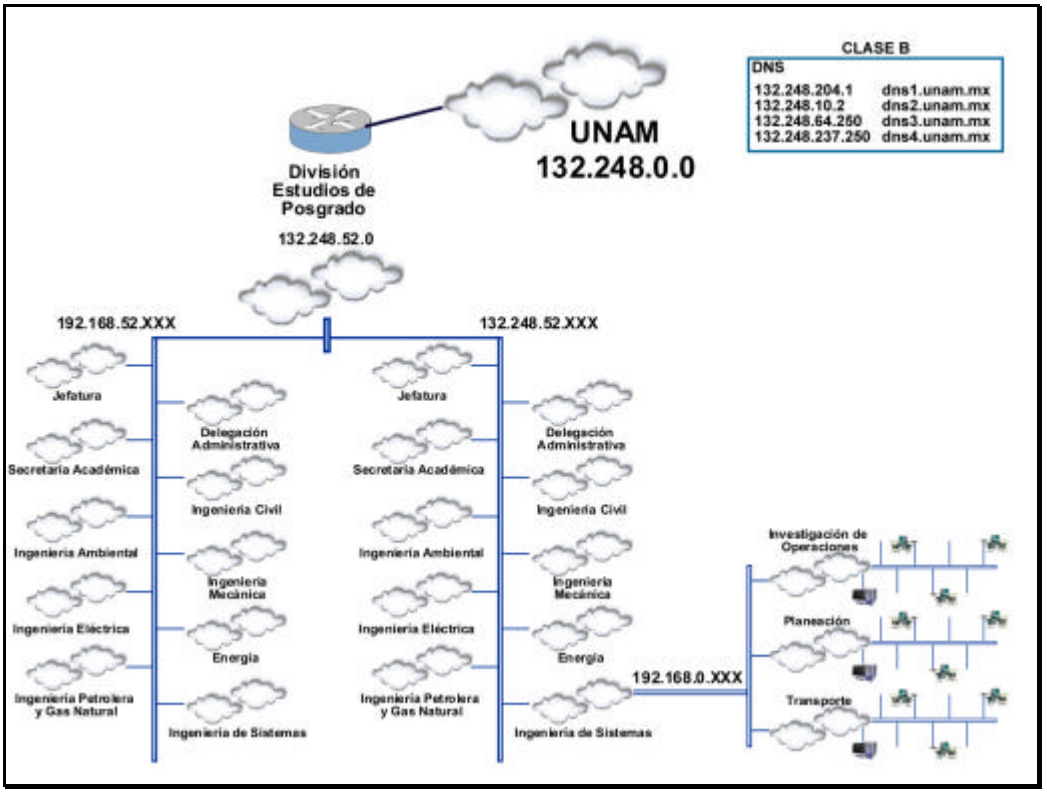


Figura 4.6 Topología lógica de la Red de Datos de la DEPFI.

4.4 Software para Medidas de Desempeño

Para el análisis del desempeño de la red, se hizo uso de algunas herramientas de software. Una de ellas es la licencia del LAN Advisor SW Edition, donada a la Facultad de Ingeniería por la empresa Agilent. Otra herramienta es el software Ntop, que tiene licencia GNU GPL y corre bajo plataforma Linux. Además se utilizó la información proporcionada por el Centro de Asistencia Técnica de REDUNAM (TAC UNAM). Se utilizaron PC's bajo el resguardo del Departamento de Sistemas de la DEPFI.

Algunas de las características de las herramientas son:

NTOP

Ntop significa Network TOP, y muestra el uso de la red. Es uno de los más completos programas de monitoreo de red. Se trata de una herramienta que permite visualizar en tiempo real los usuarios y aplicaciones que están consumiendo más recursos de red en un instante concreto, de la misma manera que la herramienta "top" de UNIX muestra los procesos que están consumiendo más CPU o memoria.

Ntop contiene dos aplicaciones:

- El Ntop clásico que contiene un servidor Web incrustado.
- Intop (Ntop interactivo) que es básicamente una interfaz de red basada en la máquina de Ntop.

Los usuarios de Ntop pueden usar un navegador Web, para navegar a través del Ntop (que actúa como un servidor Web) y obtener información del tráfico, así como un desplegado del estado de la red. En este último caso, Ntop puede ser visto como un agente RMON con una interfaz Web incrustada.

El uso de la interfaz Web, la configuración limitada, la administración vía la interfaz Web y la poca utilización de CPU y memoria hacen de Ntop fácil de utilizar y adecuado para monitorear.

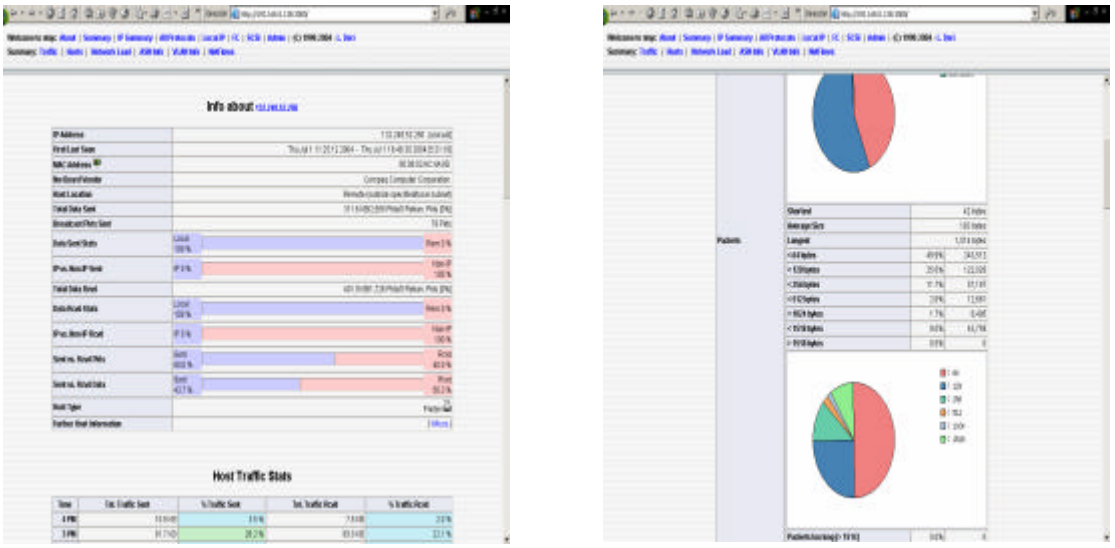


Figura 4.7 Reportes y estadísticas del Ntop.

Intop proporciona una internase poderosa y flexible pare el sniffer de paquetes Ntop. Dado que Ntop ha crecido mucho en funcionalidad y no puede ser simplemente considerado un navegador de red, el problema de capturar y mostrar la utilización de la red ha sido dividido. Como la versión 1.3 del Ntop captura paquetes, ejecuta análisis de tráfico y almacenamiento de información, Intop implementa una interfaz basada en línea de comandos con mucho de la funcionalidad ya implementada.

```
                intop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb]     Thpt: 211.9 Kbps/349.7 Kbp
 Host                  Act   -Rcvd-      Sent       TCP       UDP       ICMP
 more                  B   257.4 Kb  281.9 Kb  256.6 Kb       769          0
 zetant                B   204.2 Kb  232.3 Kb  204.2 Kb         0          0
 tar                   B    42.9 Kb   19.5 Kb   42.9 Kb         0          0
 ibook                 B    32.7 Kb    4.7 Kb   32.7 Kb         0          0
 tecserv               R       791         0         0       595        196
 bugnoli               B       602     1.4 Kb        0       602          0
 urano                 B       496     5.1 Kb        0       496          0
 utlrouter             R        98          0        0         0         98
 mis                   S         0        212        0         0          0
 fiorella              S         0        486        0         0          0
 piutltst02            S         0     1.4 Kb        0         0          0
 mostardi              S         0        952        0         0          0
 193.43.104.55         S         0        588        0         0          0
 itest1                S         0        928        0         0          0
 rolly                 S         0         46        0         0          0
 itin2                 S         0         92        0         0          0
 3comhub1              S         0        610        0         0          0
 re                    S         0     5.6 Kb        0         0          0
 pi100                 S         0     1.2 Kb        0         0          0
 lcardini              S         0        546        0         0          0
 mbeng                 S         0        602        0         0          0
 itest2                S         0        600        0         0          0
 fossati-a             S         0        960        0         0          0
 hpwsutl               S         0     3.1 Kb        0         0          0
 catlc                 S         0        120        0         0          0
 aut01b                S         0        243        0         0          0
 biu                   S         0        542        0         0          0
 artico2               S         0        226        0         0          0
```

Figura 4.8 Un reporte del Intop.

Los protocolos que es capaz de monitorear Ntop son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Las ventajas que presenta el Ntop son, entre otras:

- Ordenar el tráfico de la red de acuerdo a muchos protocolos
- Mostrar el tráfico de la red ordenado de acuerdo con varios criterios
- Desplegar estadísticas de tráfico
- Almacenar en disco estadísticas de tráfico persistente en formato RRD
- Identificar la identidad (por ejemplo, direcciones de e-mail) de los usuarios de las computadoras
- Identificar el sistema operativo del host en forma pasiva (i.e. sin enviar paquetes de prueba)
- Mostrar distribución de tráfico IP entre varios protocolos
- Analizar tráfico IP y ordenarlo de acuerdo con la fuente o destino
- Desplegar la matriz de tráfico de subred
- Reportar la utilización del protocolo IP ordenado por tipo de protocolo

En resumen, las características del Ntop son:

Plataformas	• Unix (Linux incluyendo, * DEB, Solaris, y MacOSX) • Win32 (Win95 y superiores)
Medios	• Loopback • Ethernet (802.11Q inclusive) • Token ring • PPP/PPPoE • IP • FDDI
Requisitos	• Uso De la Memoria Depende de la configuración del ntop, del número de anfitriones, y del número de las sesiones activas de TCP. En general, va de algunos MB (LAN) a 100 MB para una WAN. • Uso de la CPU Depende de la configuración del ntop, y condiciones del tráfico. En una PC moderna y una LAN grande es menos del 10% de la carga total de la CPU.
Características Adicionales	• Servidor incrustado de HTTP(S) con la ayuda de cgi • Flujos de la Red • Análisis de tráfico local • Ayuda multithread y de la P. M. (multiprocesador) en Unix y Win32 • Perl/PHP/Python API ligero para el Ntop que tiene acceso del telecontrol • Dominios de Internet (como Sistemas Autónomos), Estadística de VLAN (Lan Virtual) • Descubrimiento activo y clasificación de la red según su SO y usuarios • Decodificadores del protocolo para algunos protocolos del P2P • Protección de contraseña avanzada del HTTP del usuario con contraseñas cifradas

Es una herramienta que no puede faltar al administrador de red, porque además de monitorear todo lo que pasa en la red, es capaz de ayudarnos al momento de detectar malas configuraciones de algún equipo (esto salta a la vista porque al lado del host sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio.

Agilent Advisor

El Agilent Advisor SW Edition es un software poderoso que analiza protocolos y que ayuda a localizar fallas y a analizar redes Ethernet y Fast Ethernet.

El Advisor SW Edition se puede utilizar en una computadora personal, equipada con una tarjeta de interfaz de red en lugar del hardware Advisor LAN.

Se puede utilizar el Advisor SW para:

- Prevenir problemas de red antes de que afecten a los usuarios
- Resolver problemas de red rápida y efectivamente
- Optimizar el desempeño de la red

Algunas de las características del Advisor SW Edition son:

- Observar la robustez, utilización y actividad de los protocolos de la red
- Examinar la capa física para observar si los nodos en la red se pueden conectar y comunicar
- Observar quién está generando el mayor tráfico
- Observa qué protocolos se están utilizando
- Observa qué estaciones están estableciendo conexiones
- Encuentra qué errores de protocolos están ocurriendo en la red
- Descubre todos los nodos en la red

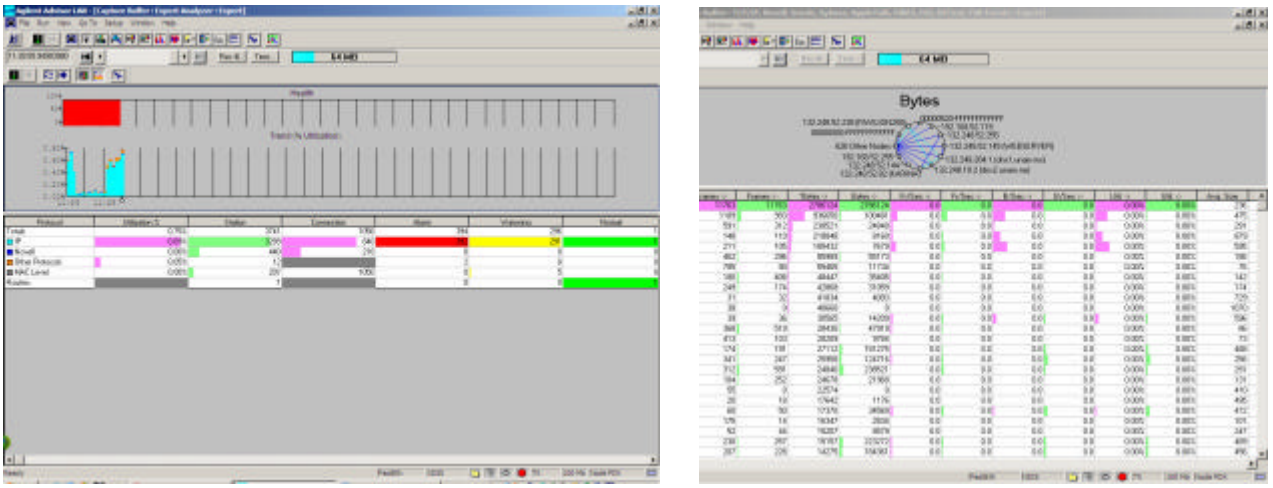


Figura 4.9 Reportes y estadísticas del Advisor SW Edition.

TAC

El Centro de Asistencia Técnica de REDUNAM proporciona información, a través de Internet, del estado de las redes LAN interconectadas a través de REDUNAM (Ver Figura 4.10). Los datos correspondientes a la DEPFI se encuentran en el grupo del nodo IIMAS-DGAE.

La información proporcionada por esta herramienta se refiere a la tasa de transmisión en diferentes escalas de tiempo (diaria, semanal, mensual y anual), así como la interfaz del equipo, el tipo de acceso al medio (CSMA/CD para Ethernet) y la velocidad del enlace.

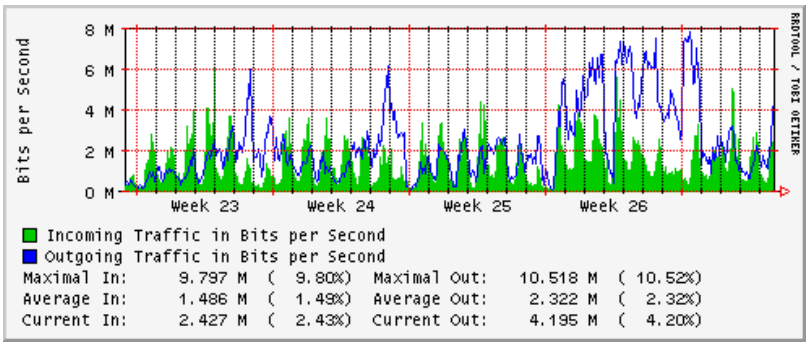


Figura 4.10 Reporte típico del TAC-UNAM

4.5 Mediciones de Desempeño

Las medidas de desempeño se realizaron en diferentes puntos de los edificios que componen la DEPFI con la herramienta Advisor SW Edition. Dichas medidas se tomaron en las fechas donde el desempeño de la red no era el adecuado, además de algunos días donde no se reportaban problemas. Las medidas tomadas con el software Ntop se registraron desde el Laboratorio de Cómputo del Departamento de Sistemas, debido a que se encuentra instalado en una PC. Se realizaron las mediciones de manera esporádica, tratando de no sesgar la muestra. Las lecturas del TAC se realizaron cuando la red presentaba problemas.

A continuación se muestran algunas de las mediciones y su interpretación.

Ntop

Las siguientes gráficas muestran el comportamiento del tráfico global de la Red.

En la Figura 4.11 se muestra la interfaz del sistema operativo donde se capturan los paquetes, el tipo de medio (Ethernet), la dirección IP del equipo que captura, su dominio y la fecha de captura.

Network Interface(s)	Name	Device	Type	Speed	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		1514	14	192.168.0.138	
Local Domain Name	localdomain							
Sampling Since	Fri Jan 12 11:12:33 2004 [5:02:00]							
Active End Nodes	243							

Figura 4.11 Reporte de Ntop: Interfaces de Red

La Figura 4.12 muestra los paquetes y los modos de transferencia. En esta lectura, la gran mayoría de los paquetes son broadcast (80.8%) mientras que para unicast, sólo el 18.9%. Esto se debe posiblemente a que los equipos están mal configurados. Este porcentaje para transferencias multicast es muy alto, y pudiera ser un factor de degradamiento de la red.

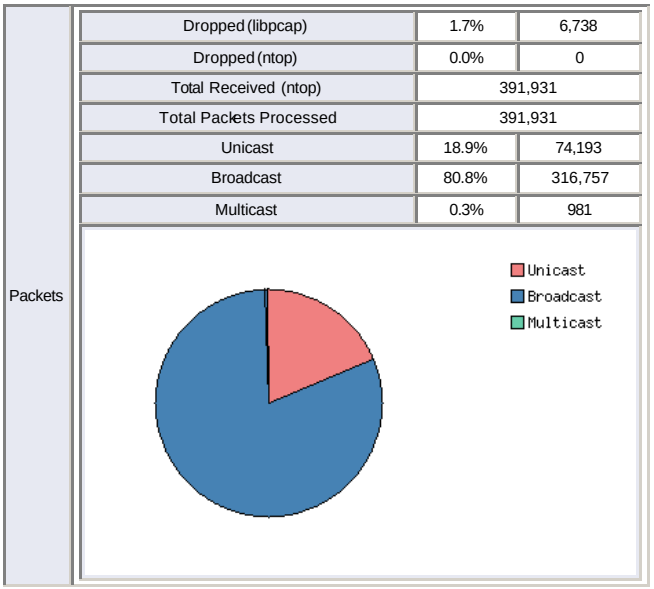
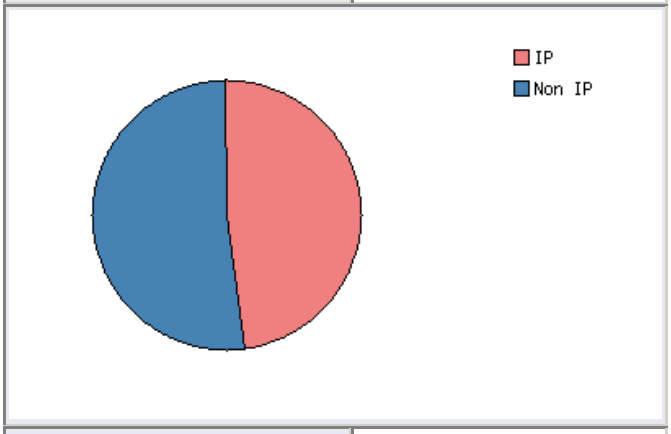


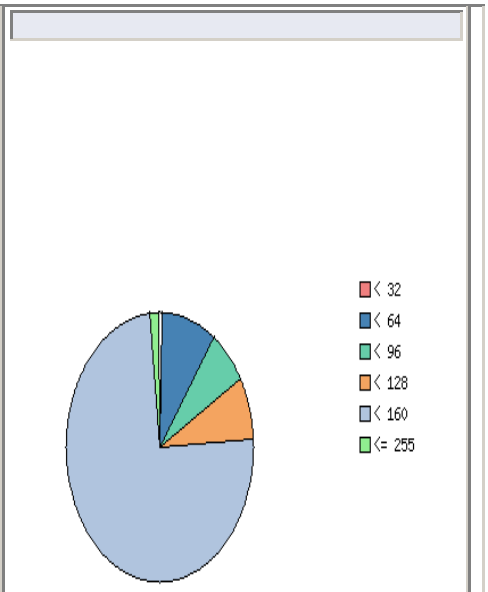
Figura 4.12 Reporte de Ntop: Paquetes y modos de transferencia

La Figura 4.13 muestra el porcentaje de tráfico IP sobre la red, así como el Tiempo de Vida de los paquetes IP (TTL). De estas lecturas podemos observar que el tráfico en la red se divide equitativamente entre paquetes IP y paquetes de otros protocolos. Así mismo, es posible observar que la mayoría de los paquetes tienen un TTL menor que 160 ms, lo que es un tiempo relativamente aceptable.

Traffic

Total	38.0 MB [38.0 MB Pkts]	
IP Traffic	18.6 MB [18.6 MB Pkts]	
Fragmented IP Traffic	0 [0.0%]	
Non IP Traffic	19.5 MB	





Average TTL	128	
TTL < 32	0.2%	749
32 < TTL < 64	2.9%	11,354
64 < TTL < 96	2.0%	7,983
96 < TTL < 128	2.3%	9,075
128 < TTL < 160	22.7%	89,126
160 < TTL < 192	0.0%	0
192 < TTL < 224	0.0%	0
224 < TTL < 256	0.4%	1,429

Protocol	Data	Percentage				
IP	18.6 MB	48.8%	TCP	5.8 MB	31%	
			UDP	11.6 MB	62%	
			ICMP	1.2 MB	6%	
			ICMPv6	3.6 KB	0%	
			IGMP	12.6 KB	0%	
			Other IP	1.3 KB	0%	
(R)ARP	9.1 MB	49%				
DLC	12.1 KB	0%				
IPX	3.9 MB	10%				
NetBios	2.8 MB	7%				
IPv6	6.1 KB	0%				
STP	526.6 KB	1%				
Other	406.7 KB	1%				

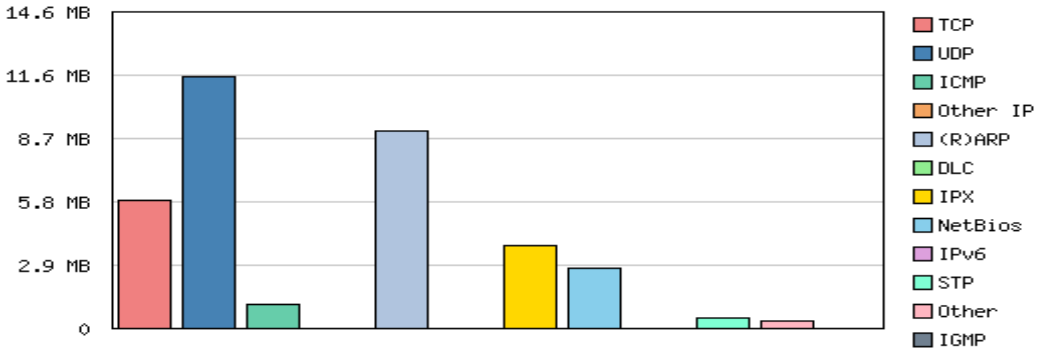


Figura 4.13 Reporte de Ntop: Distribución global de paquetes

En la Figura 4.14 se muestra la utilización de los servicios que proporcionan TCP/UDP. De aquí se observa que el protocolo NetBios sobre IP tiene una gran utilización en esta red.

TCP/UDP Protocol	Data	Percentage
HTTP	1.2 MB	6%
DNS	105.8 KB	0%
Telnet	35.8 KB	0%
NBios-IP	10.9 MB	59%
Mail	0.8 KB	0%
DHCP-BOOTP	394.1 KB	2%
Gnutella	0.3 KB	0%
Kazaa	0.1 KB	0%
eDonkey	0.2 KB	0%
Messenger	137.9 KB	0%
Other TCP/UDP-based Protocols	5.8 MB	31%

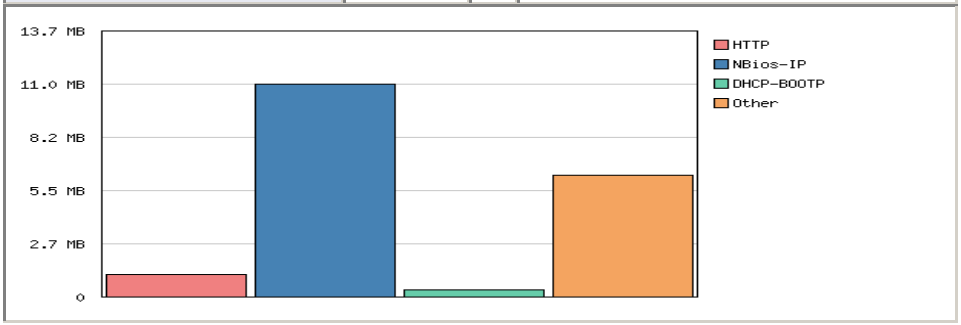


Figura 4.14 Reporte de Ntop: Distribución global de protocolos TCP/UDP

Esta gráfica muestra parte de la lectura de los hosts en la red.

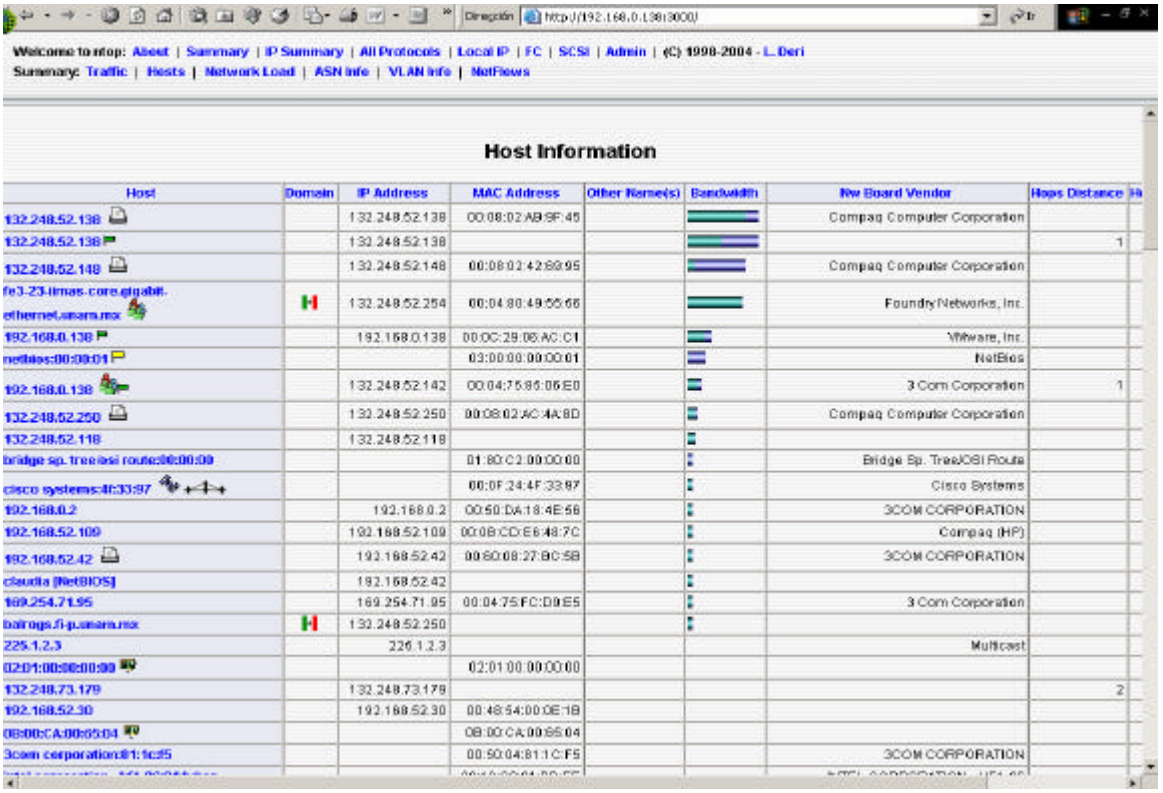


Figura 4.15 Reporte de Ntop: Información de los host.

TAC

Las siguientes gráficas muestran las tasas de transferencia de la Red de Datos de la DEPFI, vistas desde el gateway del IIMAS.

La Figura 4.16 muestra dos tipos de mediciones. La primera, es la medición diaria. En ella podemos observar que el tráfico disminuye abruptamente en horas pico (de las 15 a las 17 hrs, y de las 12 a las 14 hrs, aproximadamente), lo que nos indica que hubo una caída en la red.

La segunda medición es una semanal, en la cual se puede observar que el tráfico se mantuvo por arriba de los 2.1 Mbps, a excepción de los días lunes y martes, días en que hubo caídas de red.

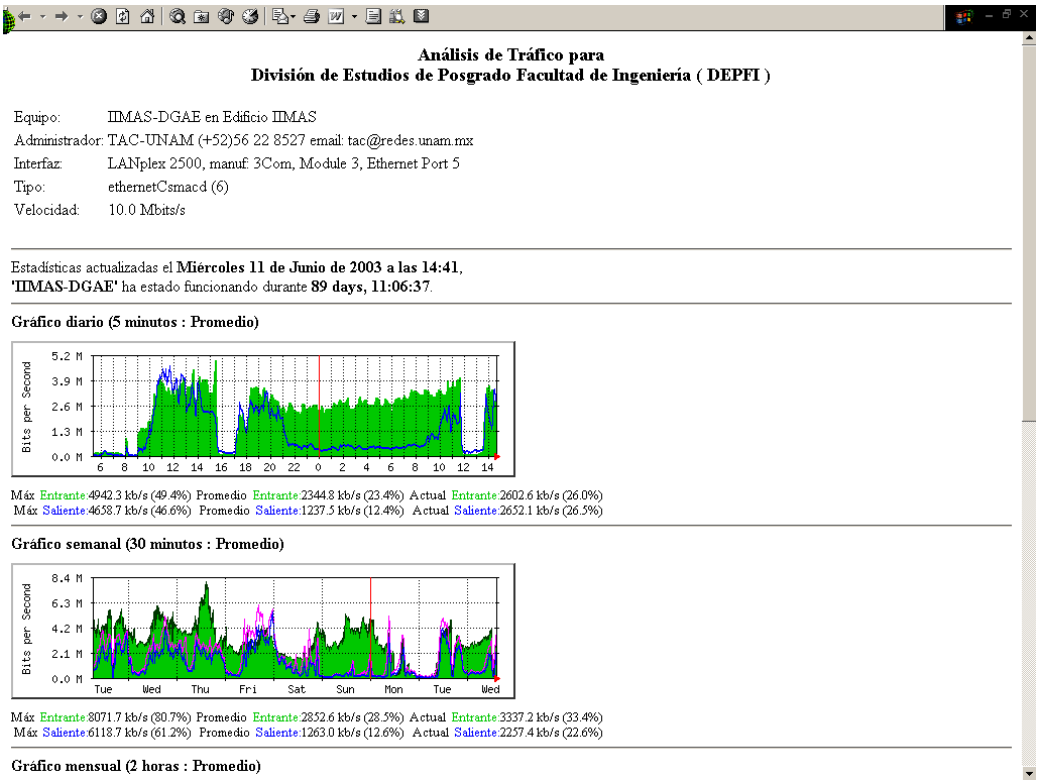


Figura 4.16 Reporte de TAC: Información diaria y semanal.

La figura 4.17 muestra la utilización mensual, en la cual el máximo de transmisión ha llegado hasta el 84.2% del ancho de banda asignado. Por otro lado, la medición anual muestra una tasa de transmisión máxima del 90%, y una media del 35%, lo que nos indica que la utilización de la red puede llegar hasta su máxima capacidad.

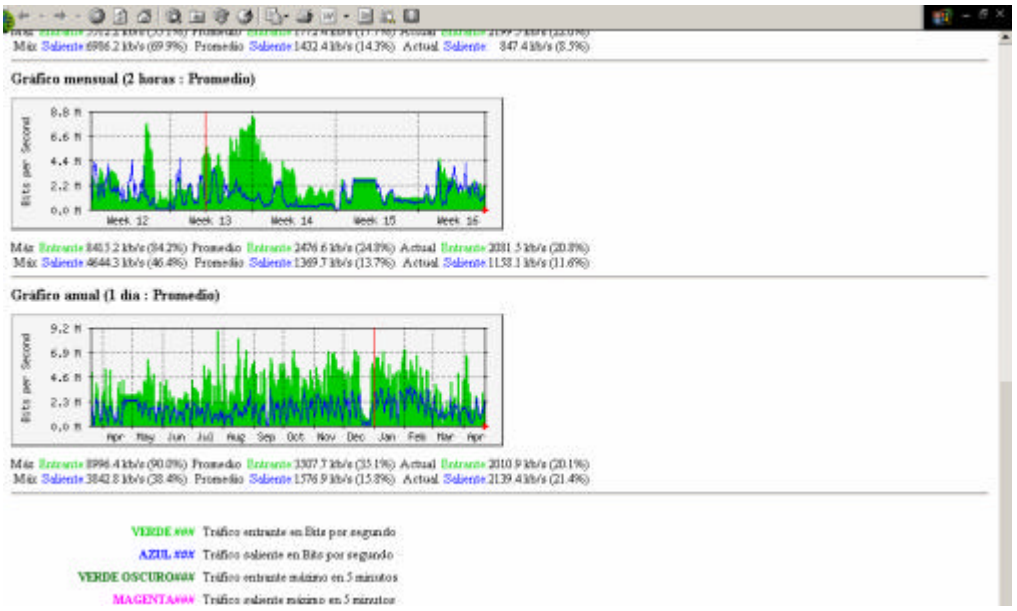


Figura 4.17 Reporte de TAC: Información mensual y anual.

Agilent SW Edition

Las siguientes figuras muestran los resultados que se obtuvieron durante el monitoreo de la red don este software. En la Figura 4.18 se ilustra el gran número de errores en el protocolo IP que se presentan en la red. Estos errores se deben a un TTL igual a cero de los paquetes enviados por los nodos en la red local, lo que significa que no hay conexión con red UNAM.

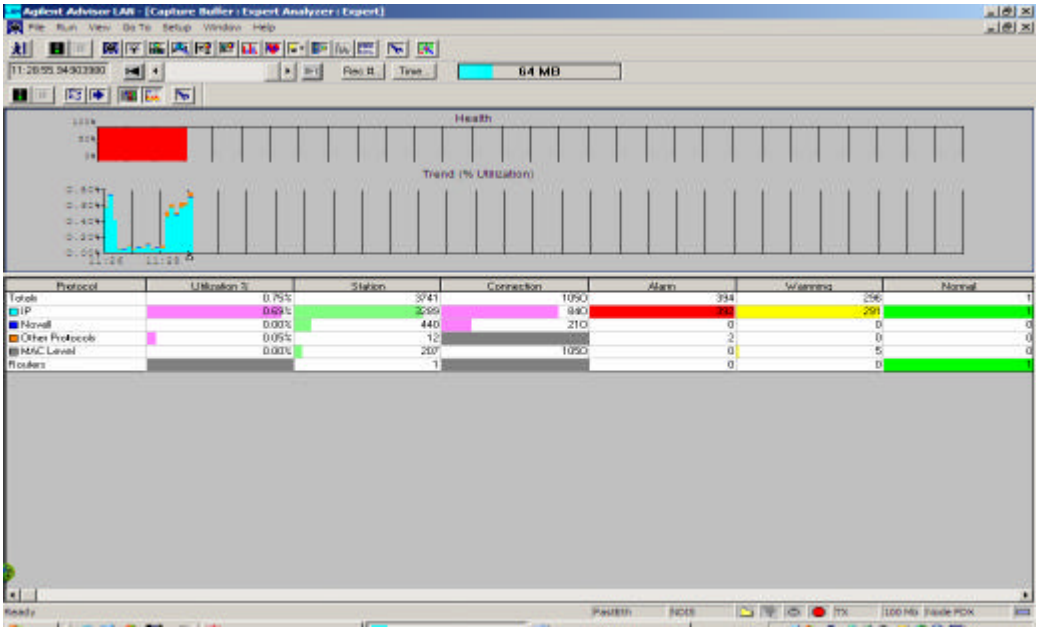


Figura 4.8 Lectura del Agilent SW Edition

En la Figura 4.19 se ilustra la alta utilización de la red por el protocolo IP, así como la historia del comportamiento en ese periodo. De ahí se observa que el número de errores IP son muchos, debidos a un TTL igual a cero. Además se observan un alto número de advertencias a nivel IP (Warnnings) que resultan de un excesivo número de retransmisiones hechas por los nodos.

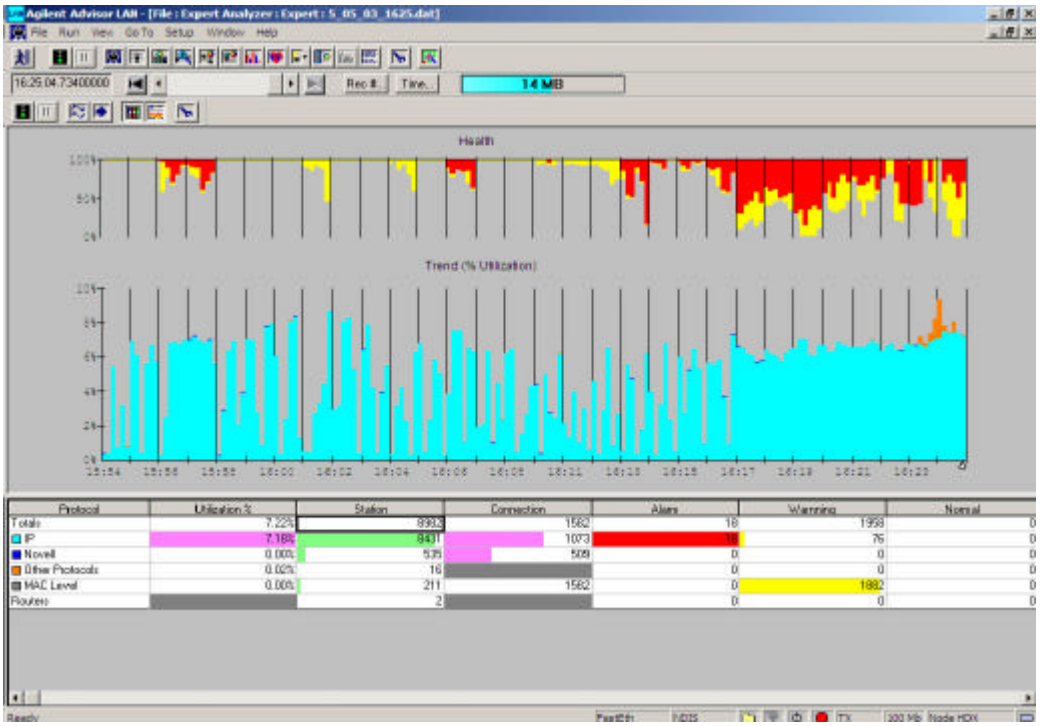


Figura 4.19 Lectura del Agilent SW Edition

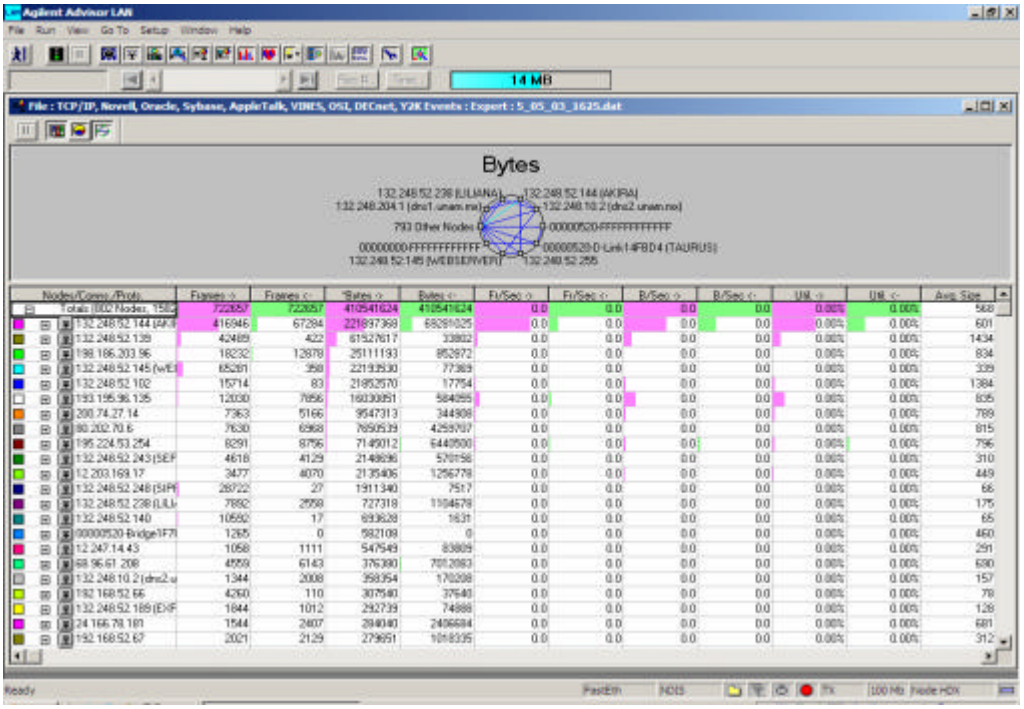


Figura 4.20 Lectura del Agilent SW Edition

4.6 Diagnóstico

Como resultado de las observaciones y mediciones realizadas en la División, pudimos encontrar los siguientes problemas:

- Desconocimiento de la ubicación del registro que contiene la fibra óptica proveniente del IIMAS. No se tienen planos y no se pudo encontrar personal en esta División ni en DGSCA que conozca la ubicación.
- No se tienen los cuidados adecuados con la fibra óptica, ya que se encuentra tirada, e incluso enredada. Este descuido podría ocasionar el mal funcionamiento de la misma (Ver Figura 4.21).
- El transceiver que recibe la señal en la acometida, no es de la División. Éste es un préstamo por parte de la DGSCA, pues el que era propiedad de la División sufrió un desperfecto.
- No hay una identificación de los cables UTP que salen de la llegada principal. (Ver Figura 4.22).
- No se encuentran bien terminados los cables UTP. Estos mismos cables ya están corroídos (cableado no estructurado).
- Los cables UTP no están en canaletas (cableado no estructurado). Ver Figura 4.23
- Canaletas flojas y sin espacio suficiente.
- Cables mal terminados.
- Falta de continuidad en algunos cables.
- Cableado a la intemperie, fuera de las canaletas instaladas.
- Cableado insuficiente para dar servicio a la demanda.
- El backbone de fibra óptica no está habilitado, hilos no rematados y algunos no funcionan (Ver Figura 4.24).

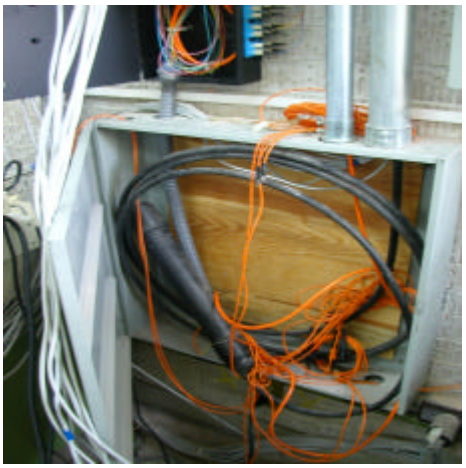


Figura 4.21 Anomalías de fibra óptica en la llegada principal

Figura 4.22 Anomalías en el cableado UTP en la llegada principal

Figura 4.23 Cables UTP sin canaletas

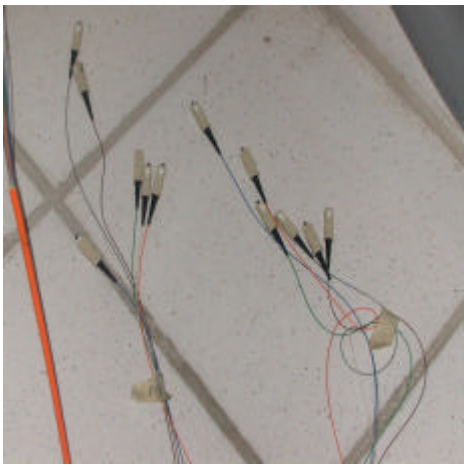


Figura 4.24 Backbone no habilitado

Además de estos problemas, existen otros catalogados como críticos: cableado estructurado, topología y administración, que a continuación se detallan.

Cableado Estructurado

Las instalaciones de la DEPFI cuentan con dos tipos de cableado, que en conjunto proporcionan el servicio de red a la División: uno que no es estructurado, previo a la construcción del Edificio Bernardo Quintana; y otro que se instaló junto con el edificio, y que es estructurado.

Los estándares EIA/TIA 568-A (Estándar de Cableado de Telecomunicaciones en Edificios Comerciales), EIA/TIA 569 (Rutas y Espacios de Telecomunicaciones), EIA/TIA 570 (Estándar de Alambrado de Telecomunicaciones Residencial y Comercial pequeño) y la Norma de Cableado Estructurado en México, son el sustento para el análisis del cableado estructurado que está presente; para el otro cableado, no se cumple ningún estándar.

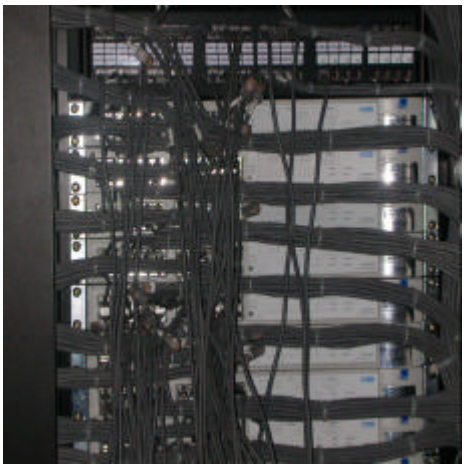


Figura 4.25 Como se puede observar en el Edificio Bernardo Quintana hay lugares en los cuales el cableado estructurado existe como tal, cumpliendo con parte de los estándares.

Subsistema Entrada del Edificio

Existe un sistema de canalización el cual provee la fibra óptica para realizar la conexión entre el backbone de REDUNAM y la DEPFI. La distancia entre ambas dependencias es menor a 200m. Se realizaron búsquedas para localizar el pozo que trae la fibra óptica que comunica al edificio, sin lograr localizarlo, por lo que no es posible saber los medios y el estado en el que el edificio la recibe. En cuanto a las vías en las que es conducida la fibra óptica, del pozo de llegada hacia el interior del edificio, y viceversa, no se puede determinar la trayectoria que siguen los ductos.

La Norma de Cableado Estructurado en México, hace mención de los dispositivos de protección que se requieren contar para los equipos que estén conectados en esta área. Cabe mencionar que en esta área de la DEPFI no se cuenta con los equipos (reguladores, no-brakes, etc.) que esta Norma recomienda. Estos equipos de protección son de gran importancia, ya que pueden prevenir de daños (por descargas eléctricas - picos) a la instalación.

Subsistema de Cuarto de Equipo

El Subsistema de Cuarto de Equipo es un espacio centralizado para los equipos de telecomunicaciones, cámaras, aparatos de protección, etc. Además debe incluir espacio de trabajo para personal de telecomunicaciones.

Como se pudo observar, en la DEPFI se carece rotundamente de este subsistema, ya que no existe un lugar físico que cumpla con las funciones antes mencionadas.

Las consideraciones que se deben tomar en cuenta para la construcción de un cuarto de equipo son descritas en los estándares y normas mencionados.

Subsistema de Cableado Horizontal

No en todas las áreas donde existe el cableado horizontal sólo se maneja cableado de datos, sino también de voz, por lo que cumple parcialmente con los estándares y la norma.

El Subsistema de Cableado Horizontal de la DEPFI cumple con: la distancia menor a 90m, se utiliza cable UTP categoría 5, los ductos a las salidas del área de trabajo sólo manejan tres cables y la ruta del cableado está fuera de interferencia electromagnética, por lo que está dentro de los estándares y la norma.

Subsistema de Cuarto de Telecomunicaciones

No existen Cuartos de Telecomunicaciones en la Biblioteca, Edificio C, ni Edificio B (ala oriente). En los límites del Edificio Bernardo Quintana con el Edificio A y el B (ala poniente), existe un cuarto de telecomunicaciones en cada piso.

En los Cuartos de Telecomunicaciones las puertas por su tamaño y funcionalidad (abren completamente); los pisos (de concreto o de loseta) con lo referente al polvo y la electricidad estática, así como la seguridad en los propio cuartos, cumplen con los estándares y la norma.

La localización de los Cuartos es la adecuada para dar servicio a los edificios A, B y Bernardo Quintana. La Biblioteca no puede ser atendida por los cuartos instalados.

No hay luces de emergencia, y en algunos casos, la instalación es defectuosa. Hay algunos racks que no tienen los 82cm de espacio de trabajo libre a su alrededor. Estos dos puntos no cumplen con los estándares y la norma.

Los tomacorrientes cumplen con el mínimo marcado por el estándar; sin embargo, en algunos cuartos son insuficientes.

Figura 4.26 Como se puede observar en el Edificio Bernardo Quintana hay Cuartos de Telecomunicaciones en los cuales el cableado estructurado existe como tal, cumpliendo con parte de los estándares.

Subsistema Cableado Vertical (Backbone)

El backbone activo de la DEPFI esta compuesto por un cable UTP categoría 5, que interconecta los Cuartos de Telecomunicaciones existentes. Este backbone es compatible con la tecnología y soporta la capacidad de los equipos conectados en los Cuartos de Telecomunicaciones.

Mientras tanto, el mismo backbone activo se conecta directamente hacia las Áreas de Trabajo, por lo que no cumple con los estándares y la norma.

El backbone inactivo, compuesto por fibra óptica, interconecta los Cuartos de Telecomunicaciones y el subsistema de Entrada del Edificio cumpliendo con las características técnicas de los equipos actuales. Este backbone sí cumple con los estándares y la norma.

Figura 4.27 se puede observar parte de la fibra óptica que no esta en funcionamiento y parte del cableado estructurado.

Subsistema del Área de Trabajo

El Subsistema de Área de Trabajo es un lugar físico que comprende las inmediaciones físicas de trabajo habitual de los usuarios.

Este subsistema debe proporcionar una salida de telecomunicaciones del punto de conexión entre el cable horizontal y los cables que conectan aparatos en el Área de Trabajo, debe instalarse un mínimo de una salida por estación de trabajo.

En la DEPFI se pudo constatar que en gran parte del edificio Bernardo Quintana se contaba con al menos un punto de conexión en las áreas de trabajo. Sin embargo, es evidente la falta de una planeación adecuada de los espacios asignados para las áreas de trabajo, ya que en algunos lugares hacen falta puntos de conexión y en otros éstos sobran.

La distribución de los puntos no fue hecha pensando en el crecimiento del número de equipos que requerirían hacer uso de la red, ya que existen zonas que no fueron consideradas para áreas de trabajo y sin embargo funcionan como tales, sin contar con puntos de conexión, y viceversa.

Topología

La topología de la red de la DEPFI es una topología de árbol. Podemos observar que la carga de la red se encuentra desbalanceada y concentrada en unos cuantos equipos (hubs).

Los equipos activos cumplen aún con su funcionalidad, pero falta poco para que lleguen a la obsolescencia. Se tiene la desventaja de que son sólo hubs y no switch's, lo que propicia que el ancho de banda decrezca conforme se agreguen usuarios. Esto lleva a que el comportamiento de la red no pueda se predecible: algunas veces es rápida, otras veces es lenta hasta el punto de caerse completamente. Debido a que se utiliza la tecnología Ethernet y que es un medio compartido, ocurren colisiones. Entre mayor sea el número de usuarios, habrá un mayor número de colisiones, y como consecuencia, se alentará la red.

Por otro lado, a nivel lógico (capa 3 del Modelo OSI) existen los problemas de la falta de administración del segmento de red proporcionado por DGSCA y falta de control de los servidores de direcciones reservadas (NAT) que instalan las diferentes Secciones del Posgrado. Esto lleva a que exista un número desmedido y poco controlado de direcciones IP dentro de la DEPFI.

Administración

La Norma de Cableado Estructurado en México establece que cada uno de los cables que conectan la salida multiusuario con los equipos debe estar correctamente identificados. Esta identificación deberá ser única, de tal forma que puedan ser localizados en cualquier momento dentro de los Cuartos de Telecomunicaciones. Estas recomendaciones no son aplicadas del todo en la Red de Datos de la DEPFI. En los Cuartos de Telecomunicaciones el cableado de los racks se encuentra identificado por cintas adheridas y en las conexiones (rosetas) de las Áreas de Trabajo. Sin embargo, existen zonas en el edificio en donde no se cuenta con la identificación de los cables, como ocurre con los cables del backbone activo. Se cumple parcialmente la Norma.

Durante este estudio se pudo constatar que no hay un control en el acceso a la acometida de red, y que continuamente se realizan alteraciones en la conexión de los equipos que aquí se encuentran. Esto ha provocado la caída en la conexión a REDUNAM. La proliferación de laboratorios y la falta de direcciones IP, dieron lugar a la creación indiscriminada de servidores NAT para satisfacer la necesidad de conexión a red, sin contar con la autorización de las autoridades.

El estándar que se refiere a la Administración para la Infraestructura de Telecomunicaciones (EIA/TIA 606) especifica los requerimientos necesarios que se deben cumplir para la administración de una red. En términos generales, de realizar la gestión de la conexión de la serie de componentes. De igual forma se refiere a la documentación que se pueda generar de dichos componentes.

En la Red de Datos de la DEPFI no se cumple con estos requerimientos, ya que no se cuenta con un administrador de red ni con personal calificado que pueda realizar y generar los registros, reportes, esquemas, documentación básica, planos actualizados, etiquetado y registros de trabajo de la operación de la red. Es de suma importancia la necesidad de tener un Administrador de Red, ya que éste podría mantener un control de toda la infraestructura de la Red de Datos de la DEPFI.

Debido a que se desconoce una gran cantidad de detalles técnicos de la Red de Datos ha sido difícil la realización del mantenimiento y actualizaciones. Tanto DGSCA como las compañías encargadas de realizar los trabajos de mantenimiento y actualización requieren de información de la infraestructura de la red, sin que hasta la fecha se cuente con ella.

Todo lo anterior es consecuencia de la falta de Administración de la Red de Datos de la DEPFI.

CAPÍTULO 5

PROPUESTAS DE ACTUALIZACIÓN Y MEDIDAS DE DESEMPEÑO.

En este capítulo se proponen acciones que logren mejorar el desempeño de la red de datos de la DEPFI, con base en sus necesidades de comunicación de datos, las tendencias de crecimiento en el uso de la red y las tecnológicas.

En la primera sección, se proponen soluciones a algunos problemas menores, descritos en el capítulo anterior. En la segunda sección se hacen dos propuestas de mejoramiento global de la infraestructura de red, teniendo como principal diferencia el cambio en los equipos activos actualmente instalados. En la última sección se muestran algunos resultados del desempeño de la red de datos, apoyándose en la actualización de uno de los equipos activos que se requirió para un proyecto de investigación de esta División, basado en Internet 2.

5.1 Propuestas de Solución a Problemas Menores

A continuación se mencionan algunos de los problemas que, a nuestro juicio, consideramos menores, dado que son fáciles de solucionar y que no tienen un gran impacto sobre el desempeño de la red de datos. Además, se dan propuestas de solución a dichos problemas.

- *Problema: Desconocimiento de la ubicación del registro que contiene la fibra óptica proveniente del IIMAS. No se tienen planos y no se pudo encontrar personal en esta División ni en DGSCA que conozca la ubicación.*

Para resolver esta falta de documentos que muestren la ubicación de los registros y la trayectoria de la fibra óptica, proponemos indagar en otras dependencias universitarias, como puede ser la Dirección General de Obras, o bien, con la(s) empresa(s) que se les dio el contrato para realizar esa obra.

- *Problema: No se tienen los cuidados adecuados con la fibra óptica, ya que se encuentra tirada, e incluso enredada. Este descuido podría ocasionar el mal funcionamiento de la misma.*

La fibra óptica deberá estar protegida dentro de un registro y estar enrollada correctamente para evitar que se dañe.

- *Problema: El transceiver que recibe la señal en la acometida, no es de la División. Éste es un préstamo por parte de la DGSCA, pues el que era propiedad de la División sufrió un desperfecto.*

Adquirir, en la medida de lo posible, el transceiver para evitar que en algún momento la DGSCA recupere su dispositivo y la DEPFI pueda continuar ofreciendo servicios. Si se realiza alguna

actualización de equipos activos en la acometida, ya no sería necesaria la adquisición de este dispositivo.

Problemas:

- *No hay una identificación de los cables UTP que salen de la acometida.*
- *No se encuentran bien terminados los cables UTP. Estos mismos cables ya están corroídos (cableado no estructurado).*
- *Cableado insuficiente para dar servicio a la demanda.*

Realizar un reacomodo de todos los cables, aplicando las recomendaciones de los estándares y la norma mexicana de cableado estructurado. Así mismo, en las áreas donde no se hace uso del cableado estructurado (en la Sección de Ingeniería Eléctrica) y se tiene cableado no estructurado, hacer uso del primero y quitar el cableado no estructurado, sobre todo, en la acometida.

Problemas:

- *Los cables UTP no están en canaletas (cableado no estructurado).*
- *Canaletas flojas y sin espacio suficiente.*
- *Falta de continuidad en algunos cables.*
- *El backbone de fibra óptica tiene hilos no rematados y algunos no funcionan.*

Realizar mantenimiento preventivo y correctivo al sistema de cableado estructurado existente, para corregir fallas en el mismo.

Recomendaciones

Para ejecutar las soluciones antes mencionadas, de manera eficaz, se podrían llevar a cabo las siguientes acciones:

- Contratar a un administrador de red, que se encargue de coordinar todas las acciones necesarias para el funcionamiento adecuado de la red.
- Contratar a alguna empresa externa a la UNAM para realizar los trabajos mayores (e.g. mantenimiento del cableado estructurado)
- Pedir a la DGO que realice los trabajos en los que tenga ingerencia (e.g. ubicación de los registros de fibra óptica)

Con estas acciones se podría imponer un orden en la estructura actual de la red de datos y un mejor control de la misma, por parte de las autoridades correspondientes. Esto beneficiaría a las autoridades para dar solución a los problemas de la red de una forma más rápida y concreta.

5.2 Actualizaciones y Mejoras

Debido a las necesidades de conexión a Internet 2, los problemas observados y las tendencias en las comunicaciones, proponemos dos proyectos de actualización global de la Red de Datos de la DEPFI, los cuales podrían realizarse por etapas, para aminorar el impacto de los costos en el presupuesto de la División. Dichos proyectos están concebidos para ser complementarios.

La realización de la Propuesta A, llevaría a un mejoramiento en el desempeño de la Red de Datos. Para poder llevar a cabo la propuesta B, es necesario contar con la actualización realizada en la Propuesta A, y además, adquirir nuevos equipos. Si sólo se desarrollara la Propuesta A, la red seguiría en funcionamiento; sin embargo, la red no estaría preparada para la demanda a mediano plazo.

Propuesta A

Con esta propuesta se pretende:

- Tener cableado estructurado en toda la DEPFI, para proporcionar un servicio confiable y de calidad de Red a todos los usuarios de la División.
- Utilizar el backbone de fibra óptica a 100 Mbps, y así aprovechar la infraestructura instalada.
- Proporcionar servicios de Internet 2, u otros servicios que requieran un ancho de banda de 100 Mbps.

Las etapas de este proyecto son:

Etapa 1. Adquisición de nuevo equipo para la acometida.

Se requiere adquirir un Switch que permita incrementar el ancho de banda de la conexión de la REDUNAM a la DEPFI de 10 a 100 Mbps, tener la capacidad de QoS, así como de baja latencia. Este switch es primordial para darle la conectividad necesaria al Proyecto "Interacción Multilateral vía Internet con Robots Cooperativos" que hace uso de Internet 2 y que se desarrolla en esta División.

Este equipo ya fue adquirido y está en operación actualmente, proporcionando un ancho de banda al enlace REDUNAM-DEPFI de 100 Mbps, así como al backbone activo. Se trata de un Switch Catalyst 2950 de 24 puertos de Cisco. Debido a la presencia de este equipo, ya no es necesaria la adquisición del transceiver antes mencionado.

El modelo Catalyst 2950 es un switch 10/100 independiente, con configuración fija y administrado, que proporciona la conectividad para redes pequeñas a medianas. Contiene las características del software Standard Image (SI) y ofrece la funcionalidad del Cisco IOS para servicios de datos, voz y video básicos.

Etapa 2. Habilitar el backbone de fibra óptica y quitar la conexión en cascada de los hubs.

Para habilitar el backbone es necesario adquirir un jumper de fibra óptica SC-MTRJ para conectar los hilos del backbone interno al switch de la llegada principal. Además, es necesario poner en operación el Core Builder, ubicado en el cuarto de Telecomunicaciones del 2° piso del Edificio Bernardo Quintana. El Core Builder distribuirá la señal proveniente de la llegada principal verticalmente, hacia los demás pisos, y horizontalmente hacia el Cuarto de Telecomunicaciones del Edificio B (ala poniente). En este Cuarto de Telecomunicaciones, es necesaria la adquisición de un Switch Cisco Catalyst 3508 con Slots de conexiones SC, para repartir la señal verticalmente.

Para quitar la conexión en cascada de los Hubs 3COM Super Stack II de los Cuartos de Telecomunicaciones de los Edificios Bernardo Quintana y B (ala poniente), es necesaria la adquisición de 30 cables de cascadeo 3C16695 de 3COM que permiten la interconexión entre hubs y formar así una sola unidad (Ver Figura 5.1).

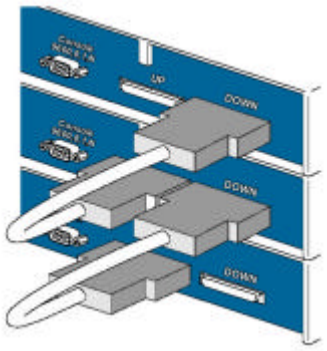


Figura 5.1 Cables para apilamiento de hubs.

Etapa 3. Cableado Estructurado.

Es necesario aplicar los estándares y la norma de cableado estructurado en las zonas de la DEPFI donde no existe. Para esto proponemos crear cuatro Cuartos de Telecomunicaciones en el ala oriente del Edificio B, uno en la Biblioteca y acondicionar el cuarto de acometida para crear un Cuarto de Equipo (Ver Figura 5.2).

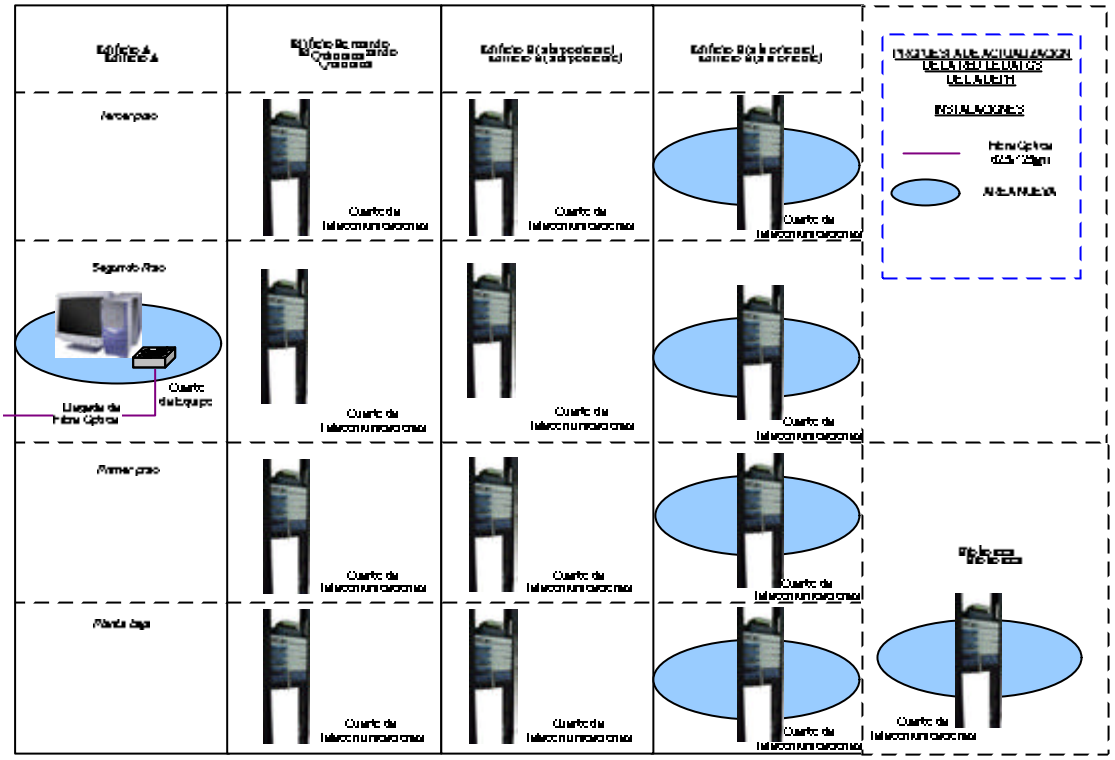


Figura 5.2 Nuevos Cuartos de Telecomunicaciones y Cuarto de Equipo

Además habrá que instalar el Cableado Horizontal en el ala oriente del Edificio B (incluyendo puntos en Áreas de Trabajo y en el Auditorio) con cable UTP categoría 5 o superior. La interfaz del Cableado Horizontal al Backbone se realizaría mediante switch's Cisco Catalyst 3550 con 24 puertos.

El Switch Catalyst 3550 es un switch apilable y multicapa, el cual proporciona alta disponibilidad, calidad del servicio (QoS) y seguridad. Tiene un amplio rango de configuraciones Fast Ethernet y Gigabit Ethernet.

Se pueden proporcionar servicios inteligentes tales como: QoS avanzado, limitación de la tasa de transmisión, administración de multicast y routing IP de alto desempeño.

Existen modelos que tienen 24 o 48 puertos 10/100 y dos puertos Gigabit Ethernet basados en GBIC, que pueden albergar transceiver GBIC tales como 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH y 1000BASE-ZX.

El Backbone en el ala oriente del Edificio B deberá ser de fibra óptica multimodo (62.5/125 µm), compatible con el backbone inactivo actual. Para interconectar el backbone en esta área con el de los demás edificios, es necesaria la instalación de un cable horizontal de fibra óptica, con las características antes mencionadas, que vaya desde el Cuarto de Telecomunicaciones del Edificio Bernardo Quintana al ala oriente del Edificio B. Será necesaria la adquisición de un Switch Catalyst 3508 de Cisco, con slots de terminales SC, que proporcionen esta conectividad.

La conexión del Backbone del ala oriente del Edificio B y la Biblioteca, se realizará a través de un LIU con conectores SC, que se encuentra en el primer piso del ala oriente del Edificio B.

La Figura 5.3 resume de manera gráfica las actualizaciones de equipo (apilamiento de hubs y adquisición de switch's) y la interconexión de todos los edificios a través de un backbone de fibra óptica a 100 Mbps.

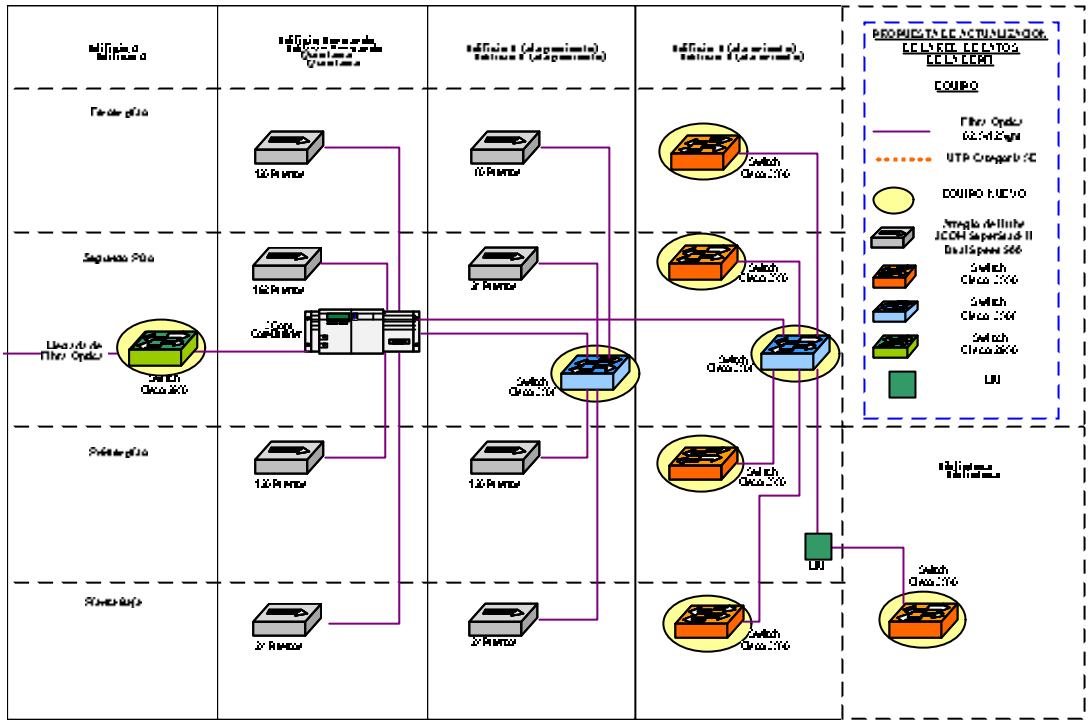


Figura 5.3 Actualización del equipo activo y del backbone de fibra óptica.

La serie Catalyst 3500 XL son switch's Ethernet 10/100 que pueden ser apilados, a los cuales es posible conectarles estaciones de trabajo y otros dispositivos de red, como servidores, routers y otros switch's. Estos switch's pueden ser desplegados como switch's de backbone, agregando tráfico 10/100 y Gigabit Ethernet desde otros dispositivos de red.

El Catalyst 3508G XL tiene las siguientes características: 8 slots 1000BASE-X basados en GBIC, soporta hasta 2500 VLAN basadas en puertos, enlaces entre switch's en todos los puertos y tiene control de tormentas broadcast para prevenir la degradación del desempeño debido a esas tormentas.

Beneficios y limitaciones.

Algunos de los beneficios de la realización de esta propuesta incluyen el cambio en la topología, con la consecuente distribución de la carga del tráfico de la red en los equipos activos propuestos y la

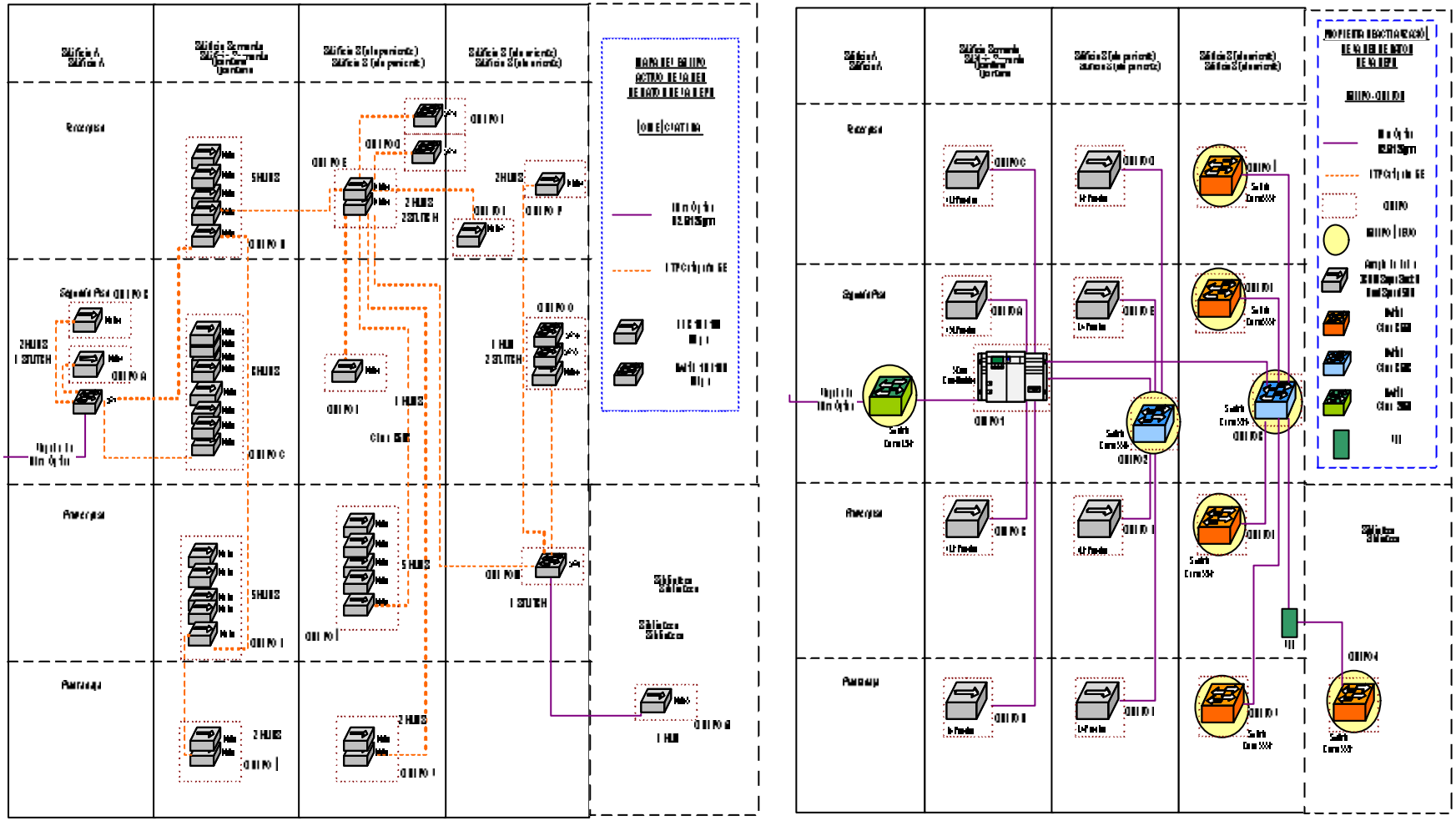
disminución de colisiones. De esta forma, los usuarios de la red tendrían beneficios, al no perder la conectividad a REDUNAM e Internet.

Además, se acondicionaría la infraestructura para posteriores servicios, como podrían ser la creación de salas de videoconferencia, el uso de redes inalámbricas, proyectos de investigación que hagan uso de Internet 2, nuevos servicios de correo electrónico, etc.

Algunas de las limitantes de este proyecto incluyen el seguir haciendo uso en gran medida de equipos viejos (Core Builder y Hubs), los cuales no han recibido mantenimiento y los modelos son obsoletos. El seguir haciendo uso de hubs implica reducir el ancho de banda final a los usuarios. Además, el ancho de banda del backbone sería de 100 Mbps, mientras que la tendencia es tener backbone Gigabit.

En la Figura 5.4 se muestra la distribución de los equipos activos y los grupos que se forman a partir de éstos, en el esquema actual y en el esquema de la Propuesta A, respectivamente. Se observa que en la Propuesta A la conexión de equipos activos se distribuye de manera más homogénea y estructurada, aunque aumenta el número de grupos.

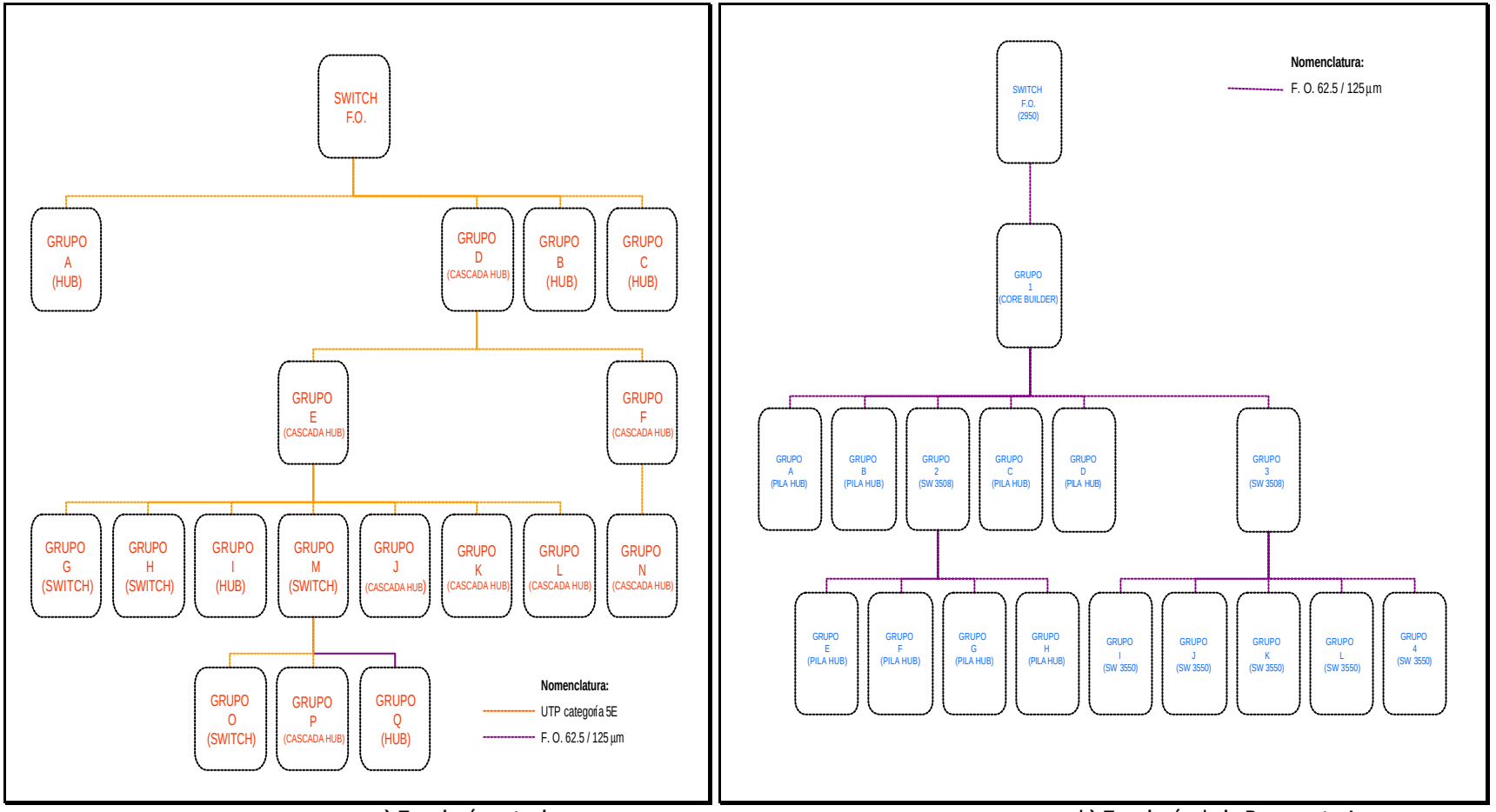
En la Figura 5.5 se muestra la topología actual y la generada con la Propuesta A. En ella, se puede observar que, aun cuando se trata de Hubs apilados en la topología propuesta, el árbol está más balanceado que en la estructura actual.



a) Esquema actual

b) Esquema de la Propuesta A

Figura 5.4 Distribución del equipo activo



a) Topología actual

b) Topología de la Propuesta A

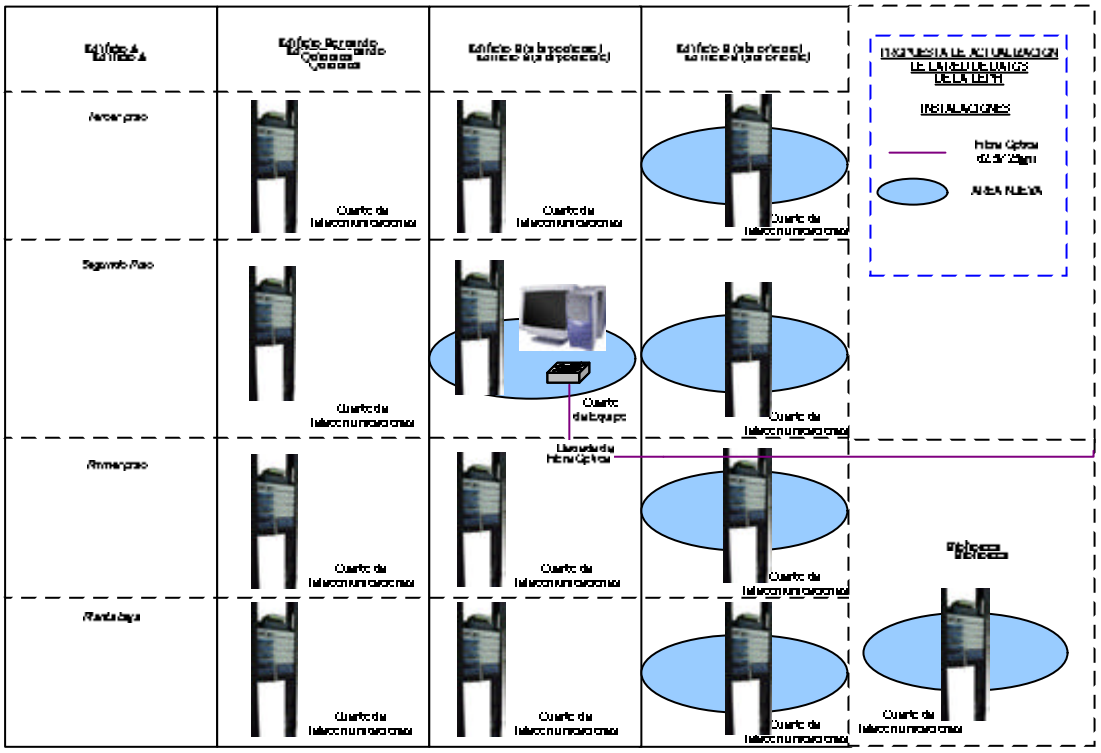
Figura 5. 5 Comparación entre topologías.

Propuesta B

Etapa 1. Quitar conexiones en cascada de los hubs, implantar un sistema de cableado estructurado en el Edificio B (ala oriente) y habilitar el backbone de fibra óptica.

Para quitar la conexión en cascada de los Hubs 3COM Super Stack II de los Cuartos de Telecomunicaciones de los Edificios Bernardo Quintana y B (ala poniente), es necesaria la adquisición de 30 cables de cascadeo 3C16695 de 3COM, que permiten la interconexión entre hubs y formar así una sola unidad (Ver Figura 5.1).

Es necesario aplicar los estándares y la norma de cableado estructurado en las zonas de la DEPFI donde no existe. Para esto proponemos crear cuatro Cuartos de Telecomunicaciones en el ala oriente del Edificio B, uno en la Biblioteca y acondicionar el cuarto de Telecomunicaciones del segundo piso del ala poniente del Edificio B para crear un Cuarto de Equipo, donde llegará la fibra óptica proveniente del IIMAS (Ver Figura 5.6).



El Backbone en el ala oriente del Edificio B deberá ser de fibra óptica multimodo (62.5/125 μm), compatible con el backbone inactivo actual. Para interconectar el backbone en esta área con el de los demás edificios, es necesaria la instalación de un cable horizontal de fibra óptica, con las características antes mencionadas, que vaya desde el Cuarto de Equipo (nuevo) del 2° piso del ala poniente del Edificio B hacia el ala oriente del Edificio B. Será necesaria la adquisición de dos Switch Catalyst 3508 de Cisco, con slots de terminales SC, que proporcionen esta conectividad.

La conexión entre el Backbone del ala oriente del Edificio B y la Biblioteca, se realizará a través de un LIU con conectores SC, que se encuentra en el primer piso del ala oriente del Edificio B y con el switch Cisco Catalyst 2950 que actualmente se utiliza para conectar la red de la DEPFI con RED UNAM.

Etapa 2. Adquisición e instalación de switch's para los Cuartos de Telecomunicaciones y la acometida.

Se adquirirá un switch Cisco Catalyst 6500 par la acometida. Este proporcionará la conectividad hacia REDUNAM y manejará el tráfico en el backbone interno. Este es el equipo que sustituirá al Core Builder.

Además, se adquirirán 8 switch Cisco Catalyst 3550 con 48 puertos y 4 con 24 puertos, para instalar uno en cada Cuarto de Telecomunicaciones. Los switch's de 48 puertos reducirán la carga de tráfico de los hubs, al hacer uso de 47 puertos destinados a dar servicio al mismo número de puntos en las Áreas de Trabajo, y un puerto para conectar a la pila de hubs (Ver Figura 5.7). En el Edificio B (ala oriente) las Áreas de Trabajo se despacharán solo con switch's de 24 puertos.

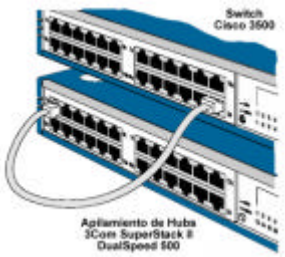


Figura 5.7 Conexión del switch y la pila de hubs, en el Cuarto de Telecomunicaciones.

La Figura 5.8 resume de manera gráfica las actualizaciones de equipo (apilamiento de hubs y adquisición de switch's) y la interconexión de todos los edificios a través de un backbone de fibra óptica a 1000 Mbps.

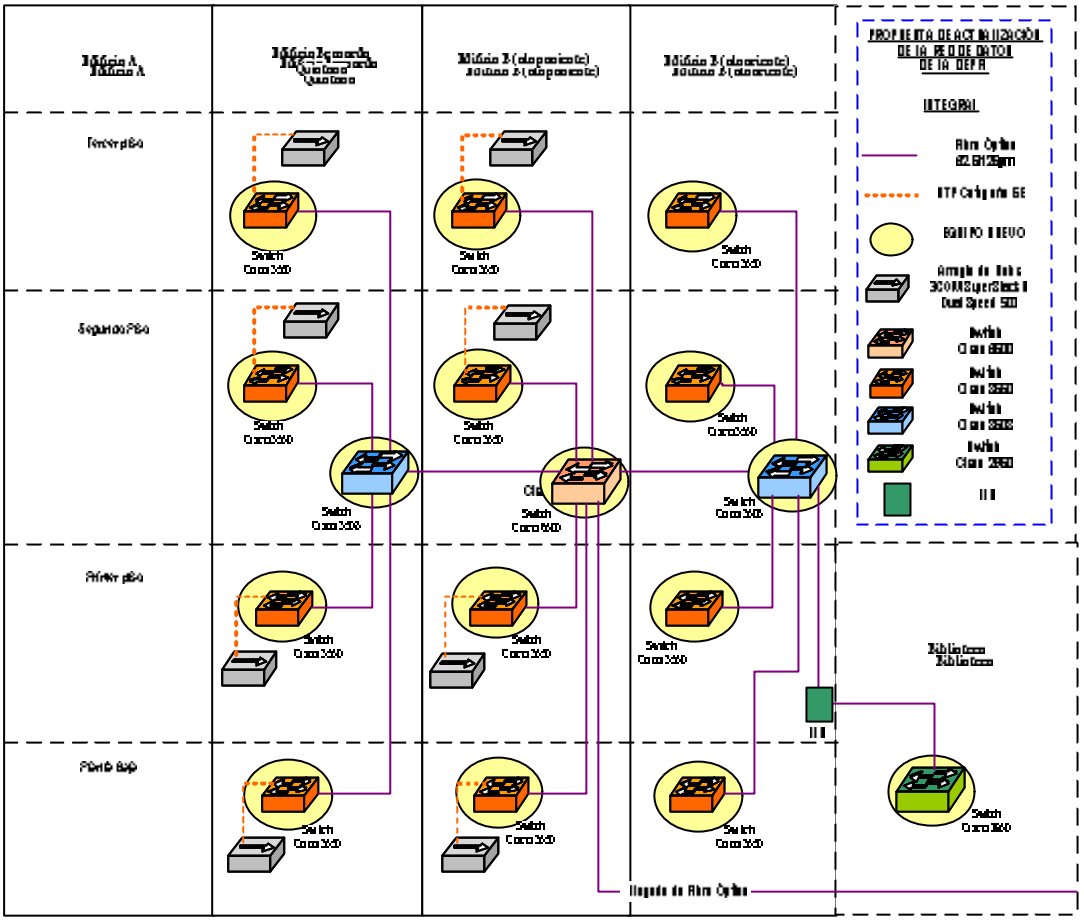


Figura 5.8 Ampliación y activación del backbone de fibra óptica

El Switch Catalyst 6500 consiste en la máquina supervisora 720, módulos de alto desempeño de 2 y 4 puertos 10 Gigabit Ethernet y 2 módulos de 48 puertos 10/100/1000 Ethernet. La nueva máquina supervisora escala el desempeño a 400 millones de paquetes por segundo para IPv4.

El módulo de 48 puertos 10/100/1000 Ethernet para Cuartos de Telecomunicaciones permite hasta 576 puertos 10/100/1000 por cada chasis, con conectividad de fábrica de 256 Gbps. Este módulo utiliza el backplane de 32 Gbps del Catalyst 6500.

Beneficios y limitaciones

Algunos de los beneficios de la realización de esta propuesta incluyen el cambio en la topología y el aumento del ancho de banda del backbone a 1Gbps, con la consecuente distribución de la carga del tráfico de la red en los equipos activos propuestos (Ver Figura 5.9). De esta forma, los usuarios de la red tendrían beneficios, al no perder la conectividad a REDUNAM e Internet y al hacer uso de un mayor ancho de banda efectivo.

En la Figura 5.10 se muestran la topología actual y la propuesta. En la Propuesta B existe un número mayor de grupos. Esto debido a que se consideraron los switch's en los cuartos de

Telecomunicaciones como un grupo extra. En esta comparación, se nota que la carga de la red está mucho más distribuida.

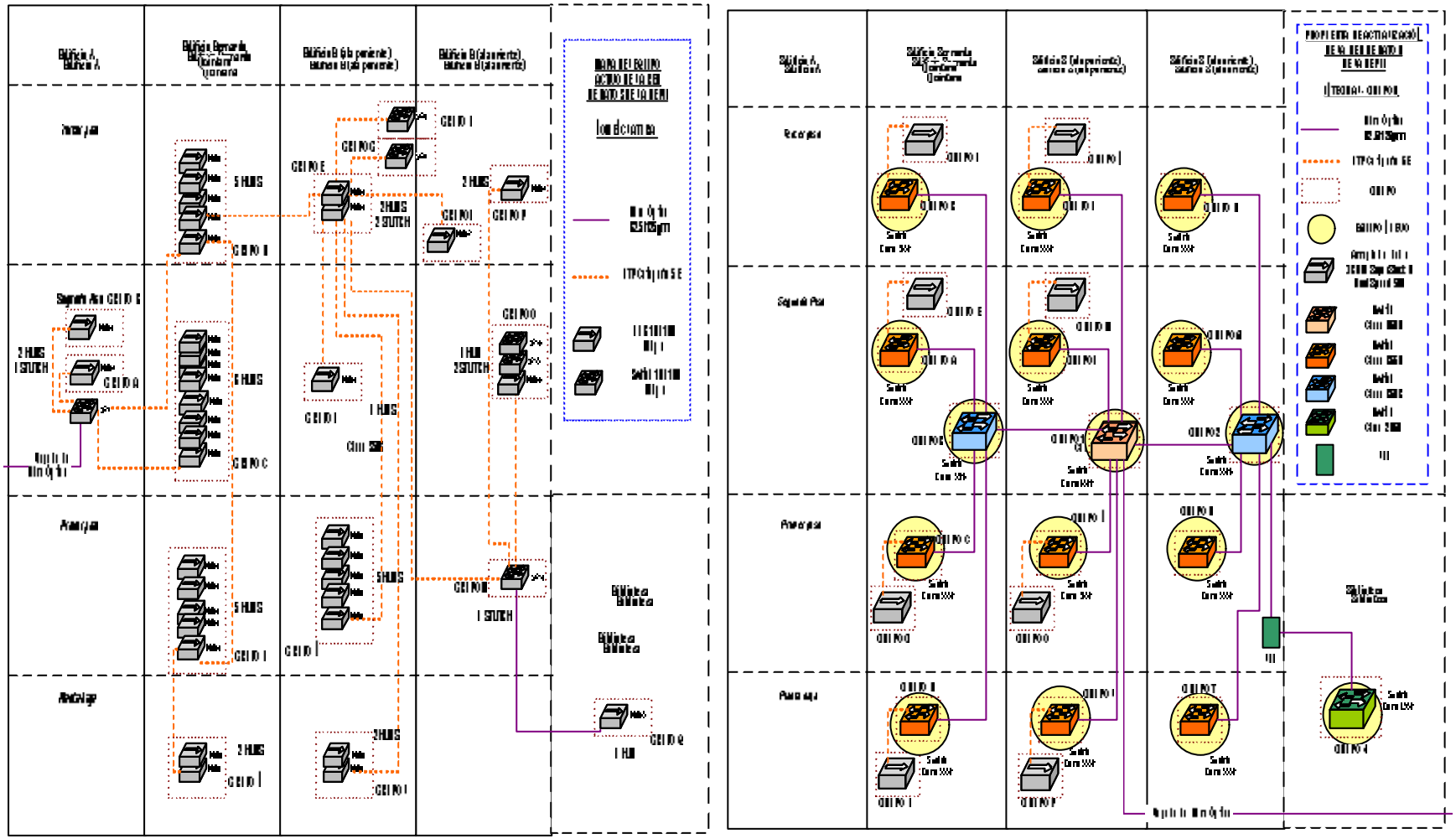
Además, se podrá segmentar la red, al hacer uso de los switch en cada Cuarto de Telecomunicaciones, creando VLANs correspondientes a las diferentes Secciones de la División; conteniendo así, el tráfico local a las Secciones y disminuyendo el tráfico global.

Este diseño pretende posicionar a la DEPFI a la vanguardia, al mantener su infraestructura actualizada y lista para las nuevas aplicaciones que demanden un gran ancho de banda, baja latencia y retardos en la transmisión, tales como la transmisión de voz, datos y video, así como el posible uso de telefonía y voz sobre IP, Internet 2, etc.

La principal desventaja de este proyecto es el alto costo en que se incurre, que para una instancia universitaria es difícil de solventar. Por ello, el cumplimiento de las etapas con un lapso de tiempo entre ellas no afectará la disponibilidad del servicio de red.

Para la realización de cualquiera de estos proyectos es importante que se cuente con el personal capacitado en el área de redes, que tenga conocimientos, habilidades y experiencia en la gestión, desarrollo y administración de proyectos de telecomunicaciones o redes de datos. La necesidad de este tipo de personal se extiende no sólo a la vida del proyecto, sino a las actividades cotidianas de administración de red de una dependencia de la importancia como la DEPFI, o aún más allá, de una institución como la UNAM.

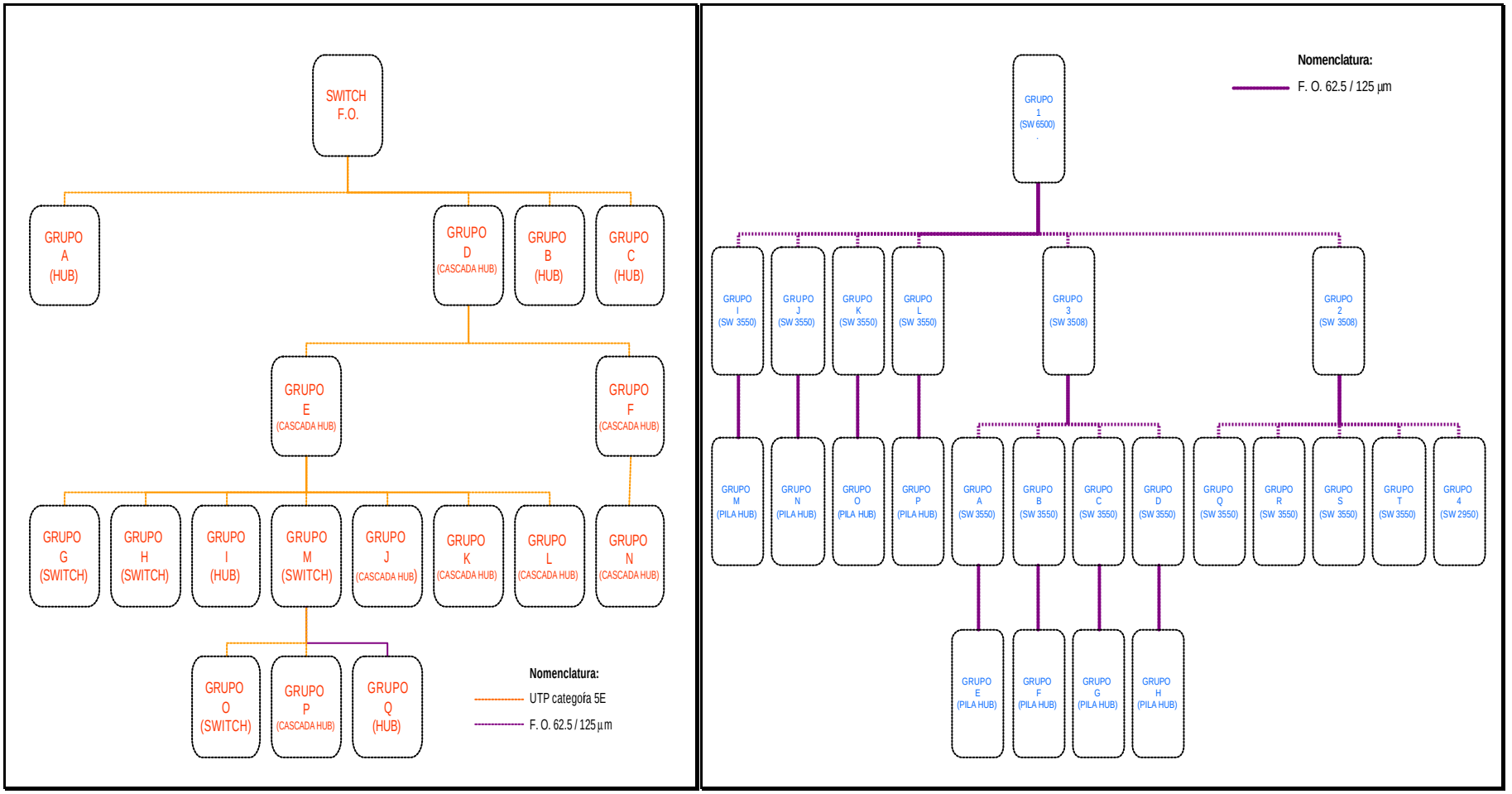
Para la solución de problemas, la planeación y el control de la red de datos de la DEPFI es de gran importancia la presencia de un Administrador de Red.



a) Esquema actual

b) Esquema de la Propuesta B

Figura 5.9 Distribución del equipo activo



a) Topología actual

b) Topología de la Propuesta B

Figura 5.10 Comparación entre topologías.

5.3 Pruebas de Desempeño

Las pruebas de desempeño de las actualizaciones realizadas a la fecha (cambio del switch de la acometida a un modelo Catalyst 2950) se pretendieron realizar con base en una aplicación específica, que hace uso de Internet 2.

El Proyecto "Interacción Multilateral vía Internet con Robots Cooperativos" consistía en "plantear la integración de una interfaz multimodal multiusuario con el propósito de realización de tareas cooperativas, utilizando robots manipuladores antropomórficos (cinemáticamente, similares a un brazo). El sistema experimental propuesto contará con dos robots en arquitectura abierta, dos cámaras, un robot haptico y un robot tipo joystick, ambos de de tres grados de libertad, y sensores de posición y de fuerza. Para propósitos de demostración, se define una tarea que requiere que uno de los robots, el robot esclavo experto ó brazo derecho, sea más hábil que el otro robot, robot esclavo inexperto ó brazo izquierdo, el cual, sujetará el objeto sobre el cual trabajará el brazo derecho. Para tal efecto, el robot esclavo experto será teleoperado bilateralmente desde una estación de telepresencia experimental del Laboratorio de Robótica y Manufactura de la Sección de Mecatrónica del CINVESTAV. El robot esclavo inexperto será tele operado virtual y unilateralmente desde el Laboratorio CENIIA de la Universidad de Guadalajara (U de G). La realización de este proyecto requiere gran ancho de banda para la efectiva estimulación bilateral de la variable de fuerza, así como el envío de las imágenes con baja latencia y pequeño retardo de transmisión. Se requieren canales diferenciados para jerarquizar las variables de control, de sensado, de monitoreo y supervisión de la tarea. Por otro lado, el retardo es crítico para la efectiva realización de la tarea, la cual no se ha llevado a cabo a nivel mundial vía Internet 1, precisamente por los problemas inherentes de retardo, de latencia aleatoria grande y ancho de banda limitado. En este proyecto se aprovecharán las ventajas que ofrece Internet 2 para implementar algoritmos avanzados de control simultáneo de fuerza y posición de robots, visión por computadora, visualización científica, visión sintética y control de robots por visión."[1]

[1] Arteaga P., Marco A. "Interacción Multilateral vía Internet con Robots Cooperativos",Formato de registro de proyectos al CUDI, marzo 2003.

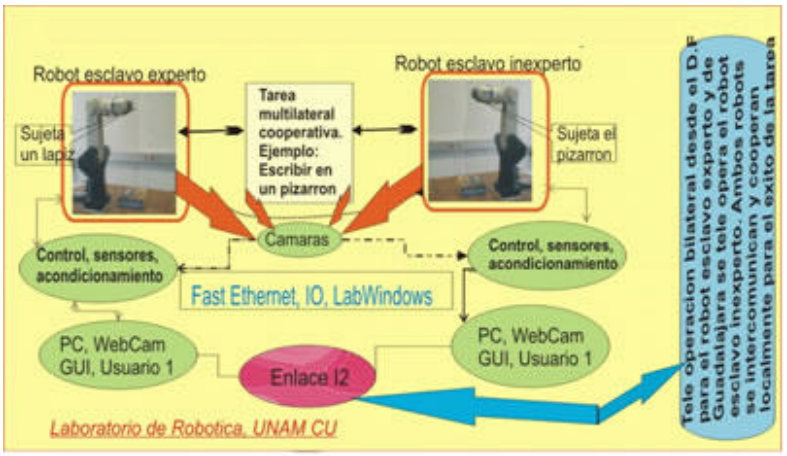


Figura 5.11 Interacción Multilateral vía Internet con Robots Cooperativos

Este proyecto tuvo los siguientes requerimientos de red:

1. "Retrasos de transmisión muy pequeños
   - ¿Cómo establecer continuamente retroalimentación multilateral de las fuerzas de contacto entre los operadores y los robots cooperativos? Tomando en cuenta que el sensor de fuerza que cierra el lazo multilateral, y que los mecanoreceptores de los operadores andan en el orden de KHz, se requiere lazos de muestreo muy rápidos en los controles locales. Por lo tanto, las referencias (posición y fuerzas de contacto) que le llegan a los lazos locales de control deben llegar con el mismo ancho de banda. Es decir se requieren retrasos de transmisión muy pequeños. La transmisión debe ser en tiempo real, sostenida durante todo el experimento, que puede durar 15 minutos, más el tiempo de inicialización y término del mismo. El retardo es quizás la variable mas crítica para la efectiva realización de la tarea, desde el punto de vista de que se requiere la implementación de algoritmos avanzados en el dominio continuo de control simultáneo de fuerza y posición de robots. De no ser así, representaría un impedimento tecnológico imposible de superar (si el retardo es considerable, digamos arriba de 100ms es muy difícil realizar una tarea inclusive mucho más sencilla de la que se está planteando en este proyecto).
2. Baja latencia
   - La estimulación visual que le llegará a cada usuario debe ser actualizada muy rápidamente, dado que estas imágenes deben ser compatibles con la estimulación kinestética que está recibiendo vía las fuerzas de contacto. Por lo tanto se requiere una latencia cercana a la frecuencia NTSC
3. Conexión permanente multipunto
   - Serán tres puntos de transmisión simultánea, dos los que están operando los robots (CINVESTAV y U de G), necesitan alto ancho de banda, mientras que la estación esclava Laboratorio de Robótica de la División de Estudios de Posgrado da la Facultad de Ingeniería de la UNAM, sólo necesita visión en línea de las WebCam

4. Enrutamiento diferenciado
    - Se requieren canales diferenciados para jerarquizar las variables de control, sensado, monitoreo y supervisión de la tarea."[2]

La importancia de este proyecto, en términos de su potencial para mejorar el uso de Internet 2 fue planteada como:

- Internet 2 se encuentra en su etapa inicial en México, y en el mundo, y el presente proyecto representa la primera aplicación multiusuario para propósitos cooperativos reales, es decir, que involucre manipulación remota multiusuario de hardware para realizar una tarea común. El potencial de aplicación de un sistema como éste para tareas de manipulación diestra, son enormes. En particular, en el sector productivo del petróleo, electricidad, medicina, entrenamiento supervisado, etcétera. Eventualmente, también, por supuesto, para propósitos de educación a distancia de laboratorios.
- Desde el punto de vista de la investigación aplicada, este proyecto permitirá la colaboración interdisciplinaria de diferentes especialistas para la exitosa consunción de un sistema avanzado de tele operación, lo cual redundará en la implantación de algoritmos avanzados de control, de informática, de robótica, de mecatrónica y de visualización científica.
- Por otro lado, este proyecto involucra la participación de estudiantes de posgrado de maestría y de doctorado como parte fundamental del desarrollo del proyecto."[3]

La instalación del switch Catalyst 2950 se llevó a cabo en marzo de 2004, un año después de haber sido aprobado el proyecto de investigación. Este hecho lamentable hizo que no se llevaran a cabo las tareas programadas para dicho proyecto, el cual culminó en abril de 2004.

Debido esta situación, no fue posible medir el desempeño de la red de Datos de la DEPFI, con tráfico IPv6. Sin embargo, se han hecho mediciones del comportamiento de la red, utilizando el LAN Advisor y Ntop, al haber aumentado el ancho de banda del backbone de 10 a 100 Mbps, teniendo un comportamiento muy diferente al observado anteriormente (Ver Figuras 5.12 y 5.13)

[2] Arteaga P., Marco A. "Interacción Multilateral vía Internet con Robots Cooperativos", Formato de registro de proyectos al CUDI, marzo 2003.
[3] Idem

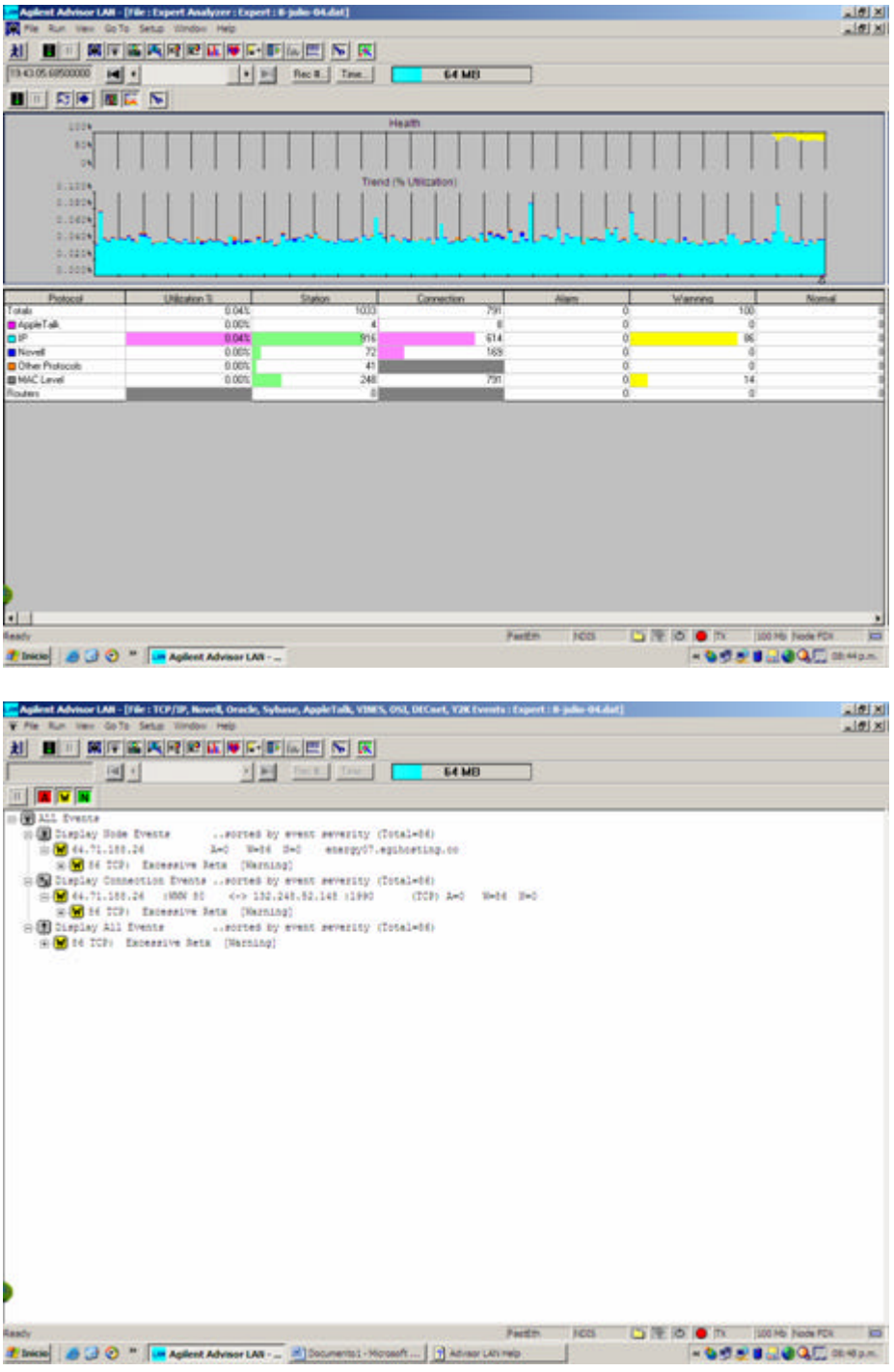
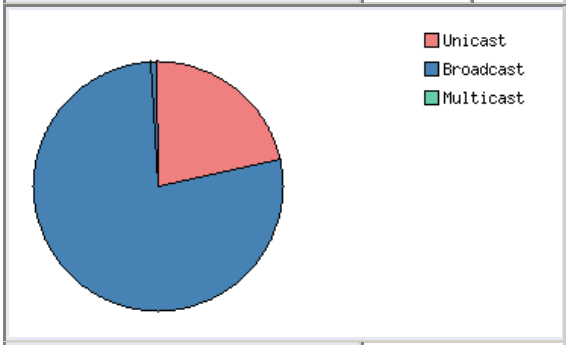
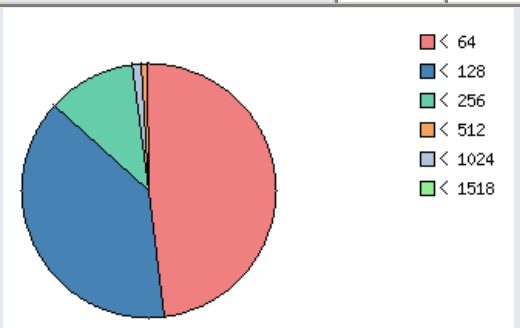
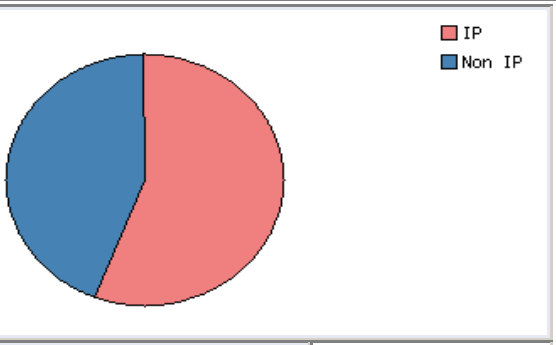
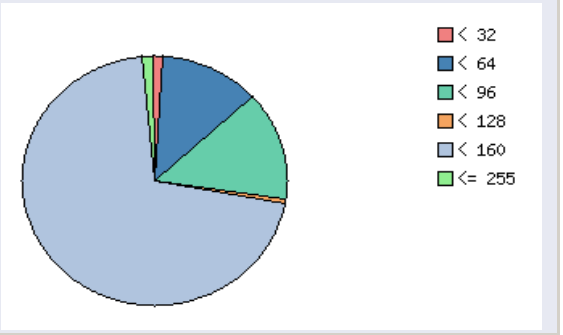


Figura 5.12 Reportes del LAN Advisor

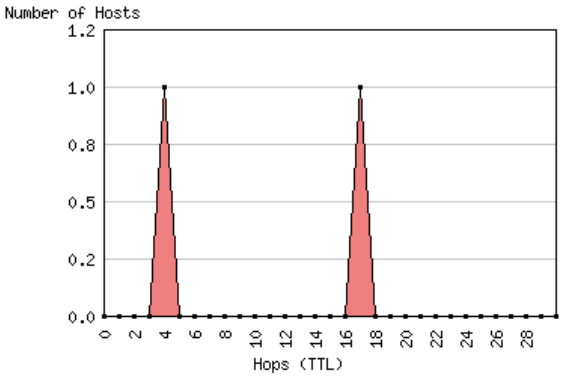
Packets	Dropped (libpcap)	178.0%	3,993
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		2,243
	Total Packets Processed		2,243
	Unicast	21.7%	486
	Broadcast	77.7%	1,742
	Multicast	0.7%	15
			
	Shortest		42 bytes
	Average Size		67 bytes
	Longest		1,514 bytes
	< 64 bytes	48.2%	1,081
	< 128 bytes	38.8%	870
	< 256 bytes	11.4%	256
	< 512 bytes	1.3%	30
	< 1024 bytes	0.0%	1
	< 1518 bytes	0.2%	5
	> 1518 bytes	0.0%	0
			
	Packets too long [> 1514]	0.0%	0
	Bad Packets (Checksum)	0.0%	0
Traffic	Total		207.3 KB [207.3 KB Pkts]
	IP Traffic		116.6 KB [116.6 KB Pkts]
	Fragmented IP Traffic		0 [0.0%]
	Non IP Traffic		90.7 KB



Average TTL		121
TTL < 32	0.5%	12
32 < TTL < 64	5.6%	125
64 < TTL < 96	6.4%	144
96 < TTL < 128	0.4%	8
128 < TTL < 160	31.6%	709
160 < TTL < 192	0.0%	0
192 < TTL < 224	0.0%	0
224 < TTL < 256	0.2%	5



Remote Hosts Distance

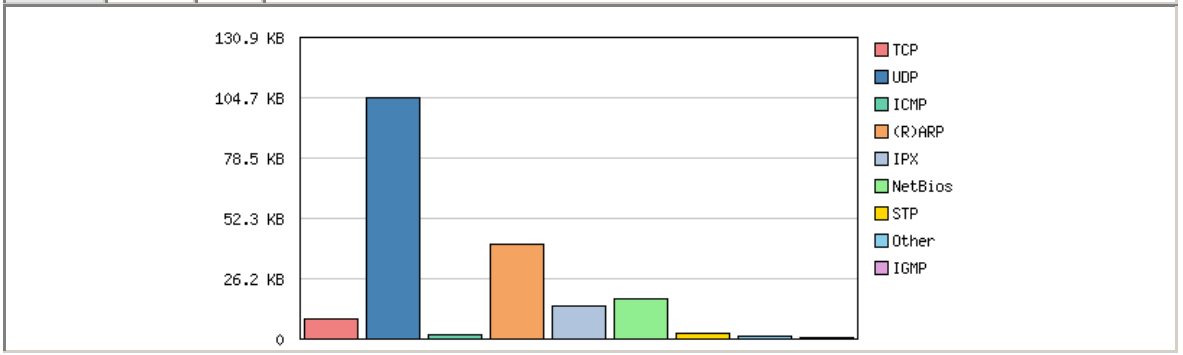


Network Load

Actual	0.0 bps	0.0 Pkts/sec
Last 5 Minutes	0.0 bps	0.0 Pkts/sec
Peak	18.6 Kbps	23.8 Pkts/sec
Average	1.9 Kbps	2.5 Pkts/sec

Global Protocol Distribution

Protocol	Data	Percentage			
IP	116.6 KB	56.3%	TCP	8.9 KB	7%
			UDP	104.7 KB	89%
			ICMP	2.3 KB	1%
			IGMP	0.7 KB	0%
(R)ARP	41.4 KB	35%			
IPX	14.7 KB	7%			
NetBios	17.5 KB	8%			
STP	2.8 KB	1%			
Other	1.6 KB	0%			



Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Percentage
HTTP	8.7 KB	7%
DNS	28.8 KB	24%
NBios-IP	73.9 KB	63%
DHCP-BOOTP	1.0 KB	0%
Other TCP/UDP-based Protocols	3.5 KB	3%

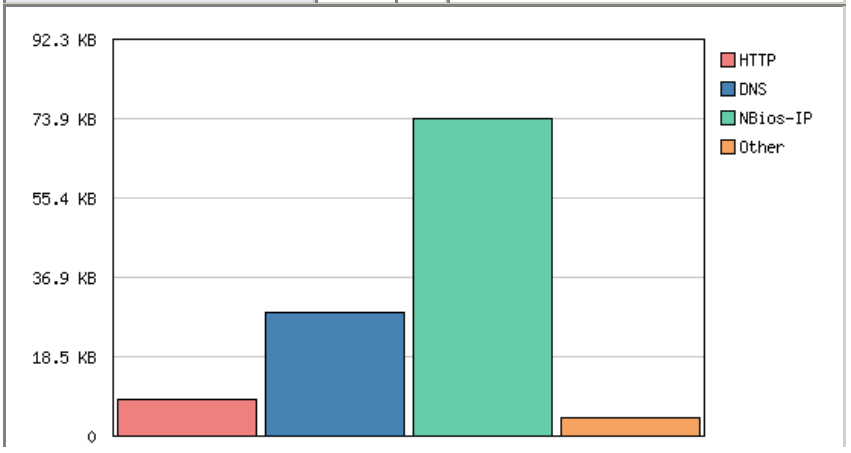


Figura 5.13 Reportes del Ntop

Las gráficas nos muestran, por un lado, que el mayor tráfico se genera con IP, y que la robustez (health) del protocolo es muy buena. Las advertencias (warnings) que se tienen en esta gráfica corresponden a un alto número de retransmisiones al puerto TCP 80.

Estas gráficas contrastan con las gráficas presentadas en el Capítulo 4, donde se muestran el agotamiento del ancho de banda y el excesivo número de errores y advertencias a nivel TCP/IP. Este resultado es producto del incremento en el ancho de banda en el backbone, así como la capacidad de manejo de paquetes que proporciona el switch Catalyst 2950.

Finalmente, estas gráficas revelan un mejoramiento ligero en el desempeño de la red de datos de la DEPFI. Sin embargo, no es completamente satisfactorio, ya que se siguen experimentando caídas frecuentes en la red, así como diversos problemas en los equipos activos.

CONCLUSIONES

La necesidad de comunicación, surgida del incremento del uso de la red de datos y el surgimiento de nuevas aplicaciones, es un factor que hace obligatoria la actualización de la infraestructura de red de la DEPFI, con el fin de proporcionar y garantizar un servicio eficiente, eficaz y de calidad en la transmisión de datos.

La falta de cumplimiento de estándares de cableado, la obsolescencia del equipo activo y la carencia de información, son factores que no permiten el aprovechamiento cabal de la infraestructura actual de la red de datos de la DEPFI.

Con la realización de este trabajo se logró recabar y generar información que es útil para la administración de la infraestructura actual. Además, se generaron propuestas de actualización que están siendo evaluadas, y en alguna medida, implantadas en la red de datos.

La Red de Datos de la DEPFI no cuenta con un administrador de red ni con personal calificado que pueda realizar y generar los registros, reportes, esquemas, documentación básica, planos actualizados, etiquetado y registros de trabajo de la operación de la red. Por tanto, es de suma importancia la necesidad de tener un Administrador de Red, ya que éste podría mantener un control de toda la infraestructura de la Red de Datos de la DEPFI.

Como producto de este trabajo, se tienen las propuestas descritas que cumplen con las necesidades y requerimientos, las cuales brindan flexibilidad ante los cambios constantes de la tecnología, en total apego a los estándares y normas de telecomunicaciones que rigen actualmente.

La ventaja de hacer una actualización es posicionar a la DEPFI a la vanguardia, al mantener su infraestructura actualizada y lista para las nuevas aplicaciones que demanden un gran ancho de banda, baja latencia y retardos en la transmisión, tales como la transmisión de voz, datos y video, así como el posible uso de telefonía y voz sobre IP, Internet 2, etc.

La principal desventaja de este proyecto es el alto costo en que se incurre, que para una instancia universitaria es difícil de solventar. Por ello, el cumplimiento de las etapas propuestas, con un lapso de tiempo razonable entre ellas no afectará la disponibilidad del servicio de red.

Asimismo, el presente trabajo podrá ser la base para futuras actualizaciones, en las cuales se puedan incorporar nuevas tecnologías (redes inalámbricas), que permitan prologar el tiempo de vida y los servicios proporcionados por la infraestructura de telecomunicaciones.

ANEXO A

POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA LA FACULTAD DE INGENIERÍA

SUBCOMITÉ DE ADMINISTRADORES DE RED

MARZO DEL 2003

POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA
LA FACULTAD DE INGENIERIA

CONTENIDO

POLÍTICAS DE SEGURIDAD EN CÓMPUTO PARA LA FI

(Marzo - 2003)

INTRODUCCIÓN

Este documento presenta las políticas de alcance institucional que permite crear y establecer una educación y una filosofía sobre la postura que en materia de seguridad en cómputo debe tener la institución respecto a los riesgos que la rodean.

Las políticas define ciertos lineamientos que establecen un límite entre lo que está permitido a los usuarios dentro de la institución y fuera de ella y lo que no está, esto es con el propósito de proteger la información almacenada en los sistemas y el acceso a éstos.

Para ello para la institución, el principio básico de seguridad es "Lo que no se permite expresamente, está prohibido".

La tecnología tiene la capacidad para abrir las puertas a un vasto mundo de recursos de información, así como de personas, a cualquier estudiante o miembro de la comunidad universitaria con una conexión a Internet. Las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así, los recursos computacionales y de conectividad disponibles. Este nuevo mundo virtual al que tenemos acceso requiere de reglas y precauciones, para asegurar un uso óptimo y correcto de los recursos. En este sentido, la Facultad de Ingeniería cree firmemente en que el desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la red de cómputo de la Facultad y el Internet un ambiente más seguro y productivo para estudiantes y miembros en general de la comunidad universitaria.

Las políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores tienen y qué hacer ante un incidente de seguridad.

Mientras las políticas indican el “qué”, los procedimientos indican el “cómo”. Los procedimientos son los que nos permiten llevar a cabo las políticas. Ejemplos que requieren la creación de un procedimiento son los siguientes:

- Otorgar una cuenta.
- Dar de alta a un usuario.
- Conectar una computadora a la red.
- Localizar una computadora .
- Actualizar el sistema operativo.
- Instalar software localmente o vía red.
- Actualizar software crítico.
- Exportar sistemas de archivos.
- Respaldar y restaurar información.
- Manejar un incidente de seguridad.

Para que esto sirva de algo, las políticas deben ser:

- Apoyadas por los directivos.
- Únicas.
- Claras (explícitas).
- Concisas (breves).
- Bien estructuradas.
- Servir de referencia.
- Escritas.
- Dadas a conocer.
- Entendidas por los usuarios.
- Firmadas por los usuarios.
- Mantenerse actualizadas.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Como administradores, nos aminoran los riesgos, y nos permiten actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. Como usuarios, nos indican la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en un sistema de cómputo, contribuyendo a que no seamos "malos vecinos" de la red sin saberlo. El tener un esquema de políticas facilita grandemente la introducción de nuevo personal, teniendo ya una base escrita y clara para capacitación; dan una imagen profesional a la organización y facilitan una auditoria.

Los principales puntos que deben contener las políticas de seguridad son los siguientes:

- Ámbito de aplicación.
- Análisis de riesgos.
- Enunciados de políticas.
- Sanciones.
- Sección de uso ético de los recursos de cómputo.
- Sección de procedimientos para el manejo de incidentes.

Al diseñar un esquema de políticas de seguridad, conviene que dividamos nuestro trabajo en varias diferentes políticas específicas: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, contabilidad del sistema, seguridad física, etc.

SEGURIDAD EN CÓMPUTO

Es un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoria.

- **Confidencial**. La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.
- **Íntegro**. La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.
- **Consistente**. el sistema, al igual que los datos, debe comportarse como uno espera que lo haga.
- **Disponible**. La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.
- **Autentificado**. Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.
- **Control de acceso**. Debe conocerse en todo momento quién entra al sistema y de dónde procede.

- Auditoria. Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

Las políticas del presente documento tienen como alcance a la Facultad de Ingeniería de la UNAM.

FACTORES CRÍTICOS

Es necesario hacer énfasis en que el apoyo por parte de la gente con el poder de decisión (cuerpo directivo) es fundamental para el éxito de un esquema de seguridad, ya que sin él, algunos elementos de dicho esquema no tendrían validez. Es vital mantener en constante capacitación al personal mediante cursos, seminarios, congresos, etc. La mejor defensa es el conocimiento. Los usuarios deben conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse así mismos de accesos no autorizados. Debe crearse una cultura de seguridad, haciendo ver a la gente involucrada los peligros a los que se está expuesto en un ambiente tan hostil como el que ha generado la evolución de las actuales redes de computadoras.

POLÍTICAS DE SEGURIDAD

La política que seguiremos será prohibitiva: "Lo que no este explícitamente permitido queda prohibido."

POLÍTICAS DE SEGURIDAD FISICA

El primer paso a considerar en un esquema de seguridad, que muchas veces no recibe suficiente atención, es la seguridad física; las medidas que se usan para proteger las instalaciones en las que reside un sistema de cómputo: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.

Políticas respecto a la seguridad física:

- Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
- Colocarlas fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastros, equipo industrial, etc.), agua, etc.
- Todos los servidores deberán ubicarse en lugares de acceso físico restringido y deberán contar para acceder a ellos con puertas con chapas.
- El lugar donde se instalen los servidores contarán con una instalación eléctrica adecuada, entre sus características con tierra física. Y dichos equipos deberán contar con NO-BREAKS.
- En los lugares donde se encuentren equipo de cómputo queda prohibido el consumo de bebidas y alimentos.
- El lugar donde se encuentre los servidores mantendrán condiciones de higiene.
- Deberá contarse con extintores en las salas de cómputo. El personal deberá estar capacitado en el uso de extintores.
- Las salas de cómputo deberán contar con una salida de emergencia.

POLÍTICAS DE CUENTAS

Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

Políticas:

- Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos. Se consideran usuarios legítimos aquellos usuarios quienes hayan realizado su tramite de registro de cuenta y que:
    1. Sean miembros vigentes de la comunidad de la Facultad de Ingeniería.
    2. Participen en proyectos especiales y tenga la autorización del jefe del área.
- Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
- La asignación de cuentas la hará el administrador del servidor del área en cuestión y al usuario sólo le dará derecho de acceder a los recursos al servidor donde se realiza el registro.
- El administrador podrá deshabilitar las cuentas que no sean vigentes.
- La cuentas y passwords personales son intransferibles.

POLÍTICAS DE CONTRASEÑAS

Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada.

Políticas:

- El administrador del servidor será el responsable de asignar las contraseñas.
- El administrador deberá contar con herramientas de detección de contraseña débiles.
- La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deberán contar con al menos seis caracteres.
- Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
- La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.
- No se podrán informar passwords por vía telefónica.
- Las contraseñas deberán cambiarse máximo cada seis meses.

POLÍTICAS DE CONTROL DE ACCESO

Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

Políticas:

- Todos lo administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
- Todos los usuarios deberán autentificarse con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.

- Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
- Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.
- Al momento de ingresar a un sistema UNIX, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema.
- El usuario tendrá el derecho a cambiar su contraseña.
- El usuario podrá utilizar los servicios de sesiones remotas si se brinda.

POLÍTICAS DE USO ADECUADO

Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido dentro del sistema de cómputo.

Existen dos enfoques: permisivo (todo lo que no esté explícitamente prohibido está permitido) y prohibitivo (todo lo que no esté explícitamente permitido está prohibido). Cuál de estas elegir dependerá del tipo de organización y el nivel de seguridad que esta requiera.

POLÍTICAS

PERMITIDO

Alumnos:

- Realizar sus tareas con fines académicos y asociadas con los programas académicos de Ingeniería.
- Utilizar los servicios de Internet donde se brinden, con fines académicos.
- Utilizar software de aplicación ya instalado.
- Utilizar los servicios de impresión donde se brinden.

Académicos, Investigadores y Administrativos.

- Utilizar el equipo de cómputo asignado para realizar sus actividades y funciones explícitamente definidas de su plaza.
- Las áreas de Investigación de Seguridad en Cómputo de la Facultad de Ingeniería (AISCFI), serán autorizadas en el subcomité de administradores de red, dichas áreas serán las únicas a las que se permitirán realizar pruebas e investigación de seguridad informática, en ambientes controlados. Las AISCFI deberán solicitar permiso e informarán de dichas pruebas al subcomité de administradores, donde se describirán del tipo de pruebas, lugar de las pruebas, fechas y horas. Cómo requisito deberán realizarse en lugares aislados (redes internas), que no comprometan la operación de las demás áreas.

PROHIBIDO

- Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.
- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aún si ésta acredita la confianza del usuario.
- Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como: programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.
- Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.
- No se permite instalar programas y software propio, en caso de requerirse deberá solicitarlo al administrador del sistema.
- No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro. Por lo cual se prohíbe descargar (o proveer) música, imágenes, videos, *chatear*, etc., con fines de ocio.

POLÍTICAS DE RESPALDOS:

PARA EL USUARIO

- Será responsabilidad del usuario mantener una copia de la información de su cuenta.

PARA EL ADMINISTRADOR DEL SISTEMA

- El administrador del sistema es el responsable de realizar respaldos de la información crítica, siempre que tenga los medios físicos para realizarla. Cada treinta días deberá efectuarse un respaldo completo del sistema. y deberá verificar que se haya realizado correctamente.
- El administrador del sistema es el responsable de restaurar la información.
- La información respaldada deberá ser almacenada en un lugar seguro.
- Deberá mantenerse una versión reciente de los archivos más importantes del sistema.
- En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.

POLÍTICAS DE CORREO ELECTRÓNICO

Establece tanto el uso adecuado como inadecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

Políticas:

- El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo, donde el administrador del sistema podrá auditar dicha cuenta.
- Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades académicos o laborales según sea el caso.
- Esta prohibido enviar correos conteniendo injurias, falsedades y malas palabras.

- Esta prohibido enviar correos sin remitente y sin asuntos.
- Esta prohibido enviar por correo virus, archivos o información que ponga en peligro la seguridad del sistema.
- Esta prohibido enviar correos SPAM.
- Esta prohibido enviar correos de publicidad personal o con intereses personales.
- Esta prohibido enviar correos haciéndose pasar por otra persona.
- Esta prohibido reenviar cadenas, chistes y toda clase de información intrascendente, ajena a la actividad académica o laboral del usuario.

POLÍTICAS DE CONTABILIDAD DEL SISTEMA

Establecen los lineamientos bajo los cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo, así como la manera en que debe manejarse la contabilidad del sistema y el propósito de la misma.

Políticas.

- El administrador del sistema deberá contar con herramientas de auditoria en el sistema.

- El administrador de red de la división o secretaría podrá realizar un monitoreo de su red, o de toda en caso de un incidente de seguridad y cuando necesite estadísticas para rediseñar su red.

- Los usuarios finales en ninguna situación podrá realizar monitoreos de la red.

- Los responsables de cómputo y el administrador general de la red tienen la autoridad de realizar auditorias internas permanentemente.

POLÍTICAS DE USO DE DIRECCIONES IP

El área responsable en representar a la Facultad de Ingeniería ante DGSCA es Secretaría General.

- El administrador de red deberá contar con un registro de sus direcciones IP utilizadas.
- El formato que utilizará para registrar su información esta contenido en el Apéndice A.
- Ningún área puede hacer uso de una dirección IP que no le corresponda, sin autorización expresa y escrita del administrador del área en cuestión.
- Ningún usuario final podrá hacer modificación en la configuración de su dirección IP asignada al equipo de su responsabilidad.
- En el campus de C.U. No se permiten el uso de servidores de DHCP con Direcciones IP homologadas.
- No se permiten utilizar en subredes de una zona, rangos de otras zonas. Por ejemplo de la en la zona A, utilizar, rangos de la zona C.
- Cada equipo que se incorpore a la red Internet deberá tener autorización del administrador de red del área en cuestión.
- Si se realiza un cambio de tarjeta de red se deberá de informar del reemplazo y de la dirección física asociada a la IP al administrador de red.
- Se permite rangos de direcciones privadas 192.168.X.X pero su asignación deberá de controlarse únicamente a los equipos asignados al área.

- Las direcciones IP que podrán otorgarse serán homologadas o privadas. Las homologadas sólo serán otorgadas si se justifican su uso y disponibilidad. Para asignar una dirección IP deberá justificarse su utilización y solicitarla al administrador o responsable de cómputo para su autorización.
- El administrador de red podrá realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.
- El administrador de red y el representante ante comité de cómputo son los únicos autorizados en solicitar dar de alta nombres canónicos de hosts, alias, mail Exchangers al Administrador General de la Red.

POLÍTICAS DE WEB.

Véase Normatividad del Web.

POLÍTICAS DE CONTRATACIÓN Y FINALIZACIÓN DE RELACIONES LABORALES DE RECURSOS HUMANOS EN SISTEMAS INFORMÁTICOS.

Políticas

- No podrán ser contratados personas como administradores de sistemas o en áreas de seguridad informática que hayan tenido responsabilidades en incidentes graves de seguridad.

- Al finalizar una relación laboral los administradores o encargados de sistemas deberán entregar todas las cuentas y passwords de los sistemas críticos.

- Los responsables de sistemas deberán cambiar todos los passwords críticos cuando un administrador de su área deje de prestar sus servicios.

SANCIONES

Al crear nuestras políticas es necesario contemplar diferentes escenarios.

Tarde o temprano, todas las políticas serán violadas. ¿Qué puede llevar a que una política sea violada?

- Negligencia.
- Error accidental.
- Desconocimiento de la misma.
- Falta de entendimiento de la misma.
-

¿Qué debemos hacer si una política es violada?

- Investigar quién llevó a cabo esta violación.
- Investigar cómo y por qué ocurrió esta violación.
- Aplicar una acción correctiva (disciplinaria).
-

¿Qué sucede si un usuario local viola las políticas de un sitio remoto?

- Debe haber acciones a seguir bien definidas con respecto a los usuarios locales.
- Debe estarse bien protegido en contra de posibles acciones desde el sitio remoto.
-

¿Cómo reaccionar ante un incidente de seguridad? Hay dos estrategias básicas:

- Proteger y perseguir
  - Su principal objetivo es proteger y preservar los servicios del sitio, y restablecerlos lo más rápido posible.
  - Se realizan acciones drásticas, tales como dar de baja los servicios, desconectar el sistema de la red, apagarlo, etc.
  - Lo utilizamos cuando:
  - Los activos están bien protegidos
    - Se correo un gran riesgo debido a la intrusión.
    - No existe la posibilidad o disposición para enjuiciar.
    - Se desconoce la base del intruso.
    - Los usuarios son poco sofisticados y su trabajo es vulnerable.
    - Los recursos de los usuarios son minados.
- Perseguir y enjuiciar
  - Su objetivo principal es permitir que los intrusos continúen con sus actividades en el sistema hasta que pueda identificarse a los responsables.
  - Lo utilizamos cuando:
    - Los recursos están bien protegidos.
    - Se dispone de respaldos confiables.
    - El riesgo para los activos es mayor que el daño de esta y futuras intrusiones.
    - El ataque proviene de un sitio con el que guardamos cierta relación, y ocurre con cierta frecuencia e intensidad.
    - El sitio posee cierta atracción para los intrusos.
    - El sitio está dispuesto a correr el riesgo a que se exponen los activos al permitir que el ataque continúe.
    - Puede controlarse el acceso al intruso.
    - Se cuenta con herramientas de seguridad confiables.
    - El personal técnico conoce a profundidad el sistema operativo y sus utilerías.
    - Existe disposición para la persecución por parte de los directivos.
    - Existen leyes al respecto.
    - En el sitio existe alguien que conozca sobre cuestiones legales.

POLÍTICAS DE SANCIONES

En caso de un incidente de seguridad grave (Un evento que pone en riesgo la seguridad de un sistema de cómputo).

Tales como:

- Obtener el privilegio de root o administrador del sistema, sin que se le haya otorgado explícitamente.
- Borrar, modificar Información.
- Difundir información confidencial.
- Copiar Información confidencial.
- Ataques maliciosos a equipos de cómputo.
- Ejecución de Programas para obtener privilegios y que sean exitosos.
- Violar correos de cuentas ajenas.

- Un incidente donde este involucrado un administrador de sistema u trabajador de la UNAM.
- Infectar intencionalmente un servidor con virus.
- Modificar Configuraciones de Switches y ruteadores sin ser responsables del equipo.
- Daño físico intencional a los medios de comunicación de la red, como fibra óptica, UTP, Switches,hubs, ruteadores, transceivers.

Si se llegase a ocurrir un incidente grave se reportará al Departamento de Seguridad de la DGSCA y se seguirán los procedimientos establecidos por ellos. Como medida precautoria y teniendo como prioridad el mantener la seguridad de los sistemas, las cuentas involucradas se deshabilitarán en toda la Facultad hasta que se deslinden las responsabilidades del incidente.

SANCIONES

Se darán las siguientes sanciones a los usuarios:

Actividad no lícita	Sanción
Consumo de alimentos, bebidas, utilización de los servicios por ocio.	Suspensión del servicio por un día. Reincidencia. Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería .
Utilizar una sesión activa ajena	Suspensión por un día su cuenta. Reincidencia. Suspensión de los servicios por un mes en todas las áreas de la Facultad de Ingeniería
Acceso con una cuenta diferente a la propia, con permiso del propietario	Suspensión por un mes de los servicios en la Facultad de Ingeniería, del que presta y del que usa la cuenta. Reincidencia. suspensión por un semestre.
Ejecución de programas que intenten adivinar cuentas y passwords locales o remotos	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. Cese definitivo de los servicios de cómputo, durante toda su carrera.
Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo propios u ajenos.	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. Cese definitivo de los servicios de cómputo, durante toda su carrera.
Hacer uso de programas que explotan alguna vulnerabilidad del sistema.	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. cese definitivo de los servicios de cómputo, durante toda su carrera.
Instalación de software externo al oficial	Suspensión del servicio por una semana. Reincidencia. suspensión por un mes.
Cambio de la configuración de los Equipos y que afecte el funcionamiento del equipo.	Suspensión del servicio por un mes.
Envíos de falsas alarmas o mensajes que atenten contra la integridad física o moral de las personas.	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. cese definitivo de los servicios de cómputo, durante toda su carrera.
Cualquier violación por parte de algún administrador de red, académico u investigador en la política de uso	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.

de direcciones IP.	
Violación de las políticas por parte de un académico, investigador, trabajador, en un incidente no grave.	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
Utilización de los servicios con fines no acordes a las funciones de su plaza en caso de ser empleado.	Carta de "extrañamiento" dirigida al Jefe de División o Secretaría.
Utilización de los servicios con fines no académicos u de ocio.	Suspensión del servicio por un día. Reincidencia. Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería .

En caso de robo y daño físico de equipo y material de forma intencional, el responsable tendrá que resarcir los daños.

La carta de extrañamiento la podrá realizar el área afectada o el subcomité de administradores de red.

PLAN DE CONTINGENCIAS.

Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. Sin embargo, ningún sistema es completamente seguro, ya que pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un *Plan de Contingencias* para "cuando falle el sistema", no "por si falla el sistema".

Políticas del Plan de Contingencias:

Todas las áreas deberán contar con un plan de contingencias para sus equipos o servicios críticos de cómputo.

A continuación mencionaremos de manera breve como realizar un plan de contingencias.

Definición de un Plan de Contingencias.

Algunas definiciones de Plan de Contingencias.

- "El plan de contingencias es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio efectuados por una paralización total o parcial de la capacidad operativa de la empresa.

  Tal estrategia, puntualizada en un manual, es resultado de todo un proceso de análisis y definiciones que dan lugar a las metodologías. A su vez las metodologías existentes versan sobre el proceso necesario para obtener dicho plan."[1]

- "Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas."[2]

[1] http://sistemas.dgsca.unam.mx
[2] BORGHELLO, Cristian F. "Seguridad Informática". 2001. Capítulo 9, página 13.

La primera definición menciona que cualquier empresa debe tener una estrategia en caso de una paralización operativa; mientras que la segunda definición es más particular, debido a que se enfoca a la Seguridad Informática, que en nuestro caso es la que nos interesa.

Pero ambas definiciones coinciden que un Plan de Contingencias debe ser capaz de reestablecer el correcto funcionamiento de la empresa o sistema y minimizar los daños.

De acuerdo con lo anterior podemos definir un *Plan de Contingencias* como:

"Conjunto de procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles."

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Se pueden analizar dos ámbitos: el primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas; y el segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado.

Fases de un Plan de Contingencia.

Fase I. Análisis y Diseño

Estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el costo/beneficio de las mismas. Ésta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión de que no es viable o es muy costoso su seguimiento. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas. Estas son llamadas *Risk Analysis* y *Business Impact*.

Las *Risk Analysis* se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Aunque los registros de incidentes son escasos y poco fiables, aún así es más fácil encontrar este tipo de metodologías que las segundas.

Las *Business Impact*, se basan en el estudio del impacto (pérdida económica o de imagen que ocasiona la falta de algún recurso de los que soporta la actividad del negocio). Estas metodologías son más escasas, pero tienen grandes ventajas como es el mejor entendimiento del proceso o el menor empleo de tiempo de trabajo por ir más directamente al problema

Las tareas de esta fase en las distintas metodologías planteadas son las siguientes:

Risk Analysis	Business Impact
1. Identificación de amenazas. 2. Análisis de la probabilidad de materialización de la amenaza 3. Selección de amenazas. 4. Identificación de entornos amenazados. 5. Identificación de servicios afectados. 6. Estimación del impacto económico por paralización de cada servicio. 7. Selección de los servicios a cubrir. 8. Selección final del ámbito del plan. 9. Identificación de alternativas para los entornos. 10. Selección de alternativas. 11. Diseño de estrategias de respaldo. 12. Selección de la estrategia de respaldo.	1. Identificación de servicios finales. 2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos no económicos. 3. Selección de servicios críticos. 4. Determinación de recursos de soporte. 5. Identificación de alternativas para entornos. 6. Selección de alternativas. 7. Diseño de estrategias globales de respaldo. 8. Selección de la estrategia global de respaldo.

Hay un factor importante a determinar en esta fase que es el *Time Frame* o tiempo que la organización puede asumir con paralización de la actividad operativa antes de incurrir en pérdidas significativas. Este factor marcará las estrategias de recuperación y se extraerá del análisis del impacto.

Fase II. Desarrollo de un plan.

Esta fase y la tercera son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.

Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la alternativa debe concluirse con la reconstrucción de la situación inicial antes de la contingencia.

Fase III. Pruebas y mantenimiento.

En esta fase se definen las pruebas, sus características y sus ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como concientizar al personal implicado.

Asimismo se define la estrategia de mantenimiento, la organización destinada a ello, y las normas y procedimientos necesarios para llevarlo a cabo.

Características de un Plan de Contingencias.

Un plan de contingencia debería de:

- Tener la aprobación de los integrantes.
- Ser flexible.
- Contener un proceso de mantenimiento.
- Tener un costo efectivo.
- Enfatizar en la continuidad del negocio
- Asignar responsabilidades específicas.
- Incluir un programa de prueba.

Aprobación.

El plan debe de ser aceptable para auditores internos; fuera de auditores, el director, clientes y proveedores.

Flexibilidad.

El plan deberá ser especificado en guías, en lugar de relacionar los detalles a situaciones individuales del desastre.

Mantenimiento.

Eludir detalles innecesarios de manera que el plan pueda ser fácilmente actualizado.

Costo-Efectividad.

La planeación del proyecto deberá enfatizar en la necesidad de minimizar los costos del desarrollo del plan, respaldo redundante del procesamiento de la suscripción de honorarios, mantenimiento y costo de pruebas.

Continuidad de la empresa.

El plan debe de asegurar la continuidad, durante un periodo de recuperación de desastres.

Respuesta organizada.

El plan debe proporcionar una lista de verificación de salidas que necesitan atención inmediata que sigue al desastre. Así mismo incluirá listas de números de teléfono y las direcciones de individuos para conectarlos.

Responsabilidad.

A individuos específicos deberá asignárseles la responsabilidad de cada salida que requiera atención durante la Respuesta de Emergencia y el tiempo del periodo del procesamiento interno.

Prueba.

La prueba con los usuarios para revisar los procedimientos de verificación de respaldo debe de realizar algo especifico en los intervalos de tiempo. De tal forma que el plan cuente con un estado de frecuencias de prueba y documente la metodología de prueba.

Características de un buen Plan de Contingencias.

- Funcional .- Desarrollado por los supervisores de primera línea.
- Costo-Efectividad .- En relación con baja probabilidad.
- Flexibilidad .- El mismo plan puede ser utilizado para cualquier desastre.
- Fácil de mantener .- Mantenerlo simple.

Pero no basta con tener un manual cuyo título sea *Plan de Contingencia* o denominación similar, sino que es imprescindible conocer si funcionará con las garantías necesarias y cubre los requerimientos en un tiempo inferior al fijado y con una duración suficiente. El plan de contingencia inexcusablemente debe:

- Realizar un análisis de Riesgos de Sistemas Críticos que determine la tolerancia de los sistemas.
- Establecer un Periodo Crítico de Recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por el que se establezcan las prioridades de Proceso.
- Determinar las prioridades de Proceso, por días del año, que indiquen cuáles son las Aplicaciones y Sistemas Críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer Objetivos de Recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de Desastre y el momento en que el Centro Alternativo puede procesar las Aplicaciones Críticas.
- Designar, entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la Capacidad de Comunicaciones.
- Asegurar la Capacidad de los Servicios de respaldos.

Algunas de las preguntas que pueden formularse al realizar una auditoria sobre este tipo de planes es:

- ¿Cómo está estructurado el Plan?
- ¿Es fácil de seguir el Plan en el caso de un desastre?
- ¿Indica el Plan quién es el responsable de desarrollar tareas específicas?
- ¿Cómo se activa el plan en caso de un desastre?
- ¿Cómo están contenidos estos procedimientos de activación en los procedimientos de emergencia normales de la organización?
- ¿Han sido probados estos procedimientos en un test de desastre simulado?
- ¿Contiene el Plan procedimientos que fijen los daños en las etapas iniciales de las Operaciones de Recuperación?
- ¿Incluye el Plan procedimientos para trasladar el proceso desde el Centro Alternativo al Centro Restaurado o Nuevo?
- ¿Contiene el Plan listados del Inventario del proceso de datos y hardware de comunicaciones, software, formularios preimpresos y stock de papel y accesorios?
- ¿Están actualizados los listados telefónicos del personal de recuperación así como empleados del proceso de datos, alta dirección, usuarios finales, vendedores y proveedores?
- ¿Cómo esta contenido el plan?
- ¿Quién es el responsable de actualizar el Plan?
- ¿Cuándo fue actualizado el plan?
- ¿Hay copias del Plan distribuidas en otro lugar?

En la auditoria es necesario revisar si existe tal plan, si es completo y actualizado, si cubre los diferentes procesos, áreas y plataformas, o bien si existen planes diferentes según entornos, evaluar en todo caso su idoneidad, así como los resultados de las pruebas que se hayan realizado, y si permite garantizar razonablemente que en caso necesario, y a través de los medios alternativos, propios o contratados, podría permitir la reanudación de las operaciones en un tiempo inferior al fijado por los responsables del uso de las aplicaciones, que a veces son también los propietarios de las mismas pero podrían no serlo.

Si las revisiones no aportan garantías suficientes se deben sugerir pruebas complementarias o hacer constar en el informe, incluso indicarlo en el apartado de limitaciones.

Es necesario verificar que la solución adoptada es adecuada: instalaciones propias, ajenas, compartidas, etc. Y que existe el contrato oportuno si hay participación de otras entidades aunque sean del mismo grupo o sector.

Dentro de lo crítico de las aplicaciones se puede distinguir entre las más críticas, con impacto muy alto en el negocio y sin alternativa, otras con alternativas, e incluso diferenciado si con costos altos o inferiores, y aquellas cuya interrupción, al menos en un número de días fijado, no tiene casi incidencia y habrá que distinguir qué tipos de consecuencias e impacto, en función del sector y entidad, y día del mes en que ocurriera el incidente, y tal vez la hora en algunos casos. Frente a lo que venía siendo la previsión de contingencias en estos años pasados, centrándose sólo en el host como un gran servidor, hoy en día, con la clara tendencia a entornos distribuidos, es necesario considerar también estos en la previsión de las contingencias.

Debe existir un manual completo y exhaustivo relacionado con la continuidad en el que se contemplen diferentes tipos de incidencias y a que nivel se puede decidir que se trata de una contingencia y de qué tipo.

En términos generales, el Plan de Contingencias deberá contener:

- Objetivo del Plan de Contingencias: Se deben indicar aquellos componentes de la función crítica que se pretenden cubrir frente a la contingencia considerada. Estos componentes pueden variar, así como su grado de cobertura para las distintas contingencias analizadas.

- Criterio para la ejecución del Plan de Contingencias: Condiciones bajo las cuales se considera que debe comenzar a aplicarse el Plan de Contingencias.

- Tiempo esperado de duración del Plan de Contingencias: Es el tiempo máximo que se puede continuar operando bajo estas condiciones de contingencia.

- Roles, responsabilidad y autoridad: Esto es dave para la buena marcha del Plan de Contingencias. Se debe determinar muy claramente, cuál es el papel de cada uno de los sectores de la organización ante la contingencia y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de contingencia.

- Requerimientos de recursos: Qué recursos se necesitan para operar en el modo contingencia y cuáles de los recursos habitualmente utilizados no se deben utilizar. Esto debe estar debidamente documentado y verificado lo más exhaustivamente posible.

- Capacitación: Otro aspecto importante es la capacitación al personal que debe intervenir en la contingencia, cuando ésta se presente. Es necesario que el personal involucrado sepa cómo se saca de servicio cualquier componente que, según el Plan de Contingencias, no debe seguir operando ante alguna falla; que pueda darse cuenta de qué debe hacer y que esté en capacidad de hacerlo cuando sea preciso. También debe tenerse en cuenta que en algún momento habrá que volver a la operación habitual; por lo tanto deberán incluirse en el plan de mecanismos para volver a la operatoria anterior a la contingencia y el tiempo máximo que la función puede permanecer en estado de contingencia.

- Implementación y Operación de los Planes de Contingencia: Se desea que no haya que implementar los Planes de Contingencia, sin embargo, por si esto sucede, hay que estar preparado y tener instructivos claros para todas las tareas que deberían realizarse.

- Reinstalación: La contingencia como su nombre lo indica, no es una situación permanente. Por lo tanto, se deben prever mecanismos como para recuperar los datos de operación durante la contingencia, si es que son

necesarios, y para aplicar las instrucciones necesarias para que las operaciones no sufran una interrupción traumática al terminar el periodo de contingencia.

ÉTICA INFORMÁTICA.

La ética se define como: "principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos, y la moral." [3]

Es conveniente diferenciar la ética de la moral, la ética es una disciplina filosófica, la cual tiene como objeto de estudio la moral, esto no quiere decir que la ética crea la moral, sino solamente reflexiona sobre ella.

"La moral se refiere a la conducta del hombre que obedece a unos criterios valorativos acerca del bien y el mal, mientras que la ética reflexiona acerca de tales criterios, así como de todo lo referente a la moralidad." [4]

Otro concepto importante es el de valor, este no lo poseen los objetos por si mismo, sino que estos lo adquieren gracias a su relación con el hombre como ser social. [5]

Definiciones de la Ética Informática.

La *Ética de la Informática* (EI) es una nueva disciplina que pretende abrirse campo dentro de las éticas aplicadas. El origen remoto de la EI está en la introducción masiva de las computadoras en muchos ámbitos de nuestra vida social. Muchas profesiones reivindican para sí una ética particular con la cual pueden regirse ante los problemas morales específicos de esa profesión o actividad ocupacional. La existencia de la EI tiene como punto de partida el hecho de que las computadoras suponen unos problemas éticos particulares y por tanto distintos a otras tecnologías. En la profesión informática se quiere pasar de la simple aplicación de criterios éticos generales a la elaboración de una ética propia de la profesión. Los códigos éticos de asociaciones profesionales y de empresas de informática van en esta dirección.

La definición más restrictiva de la EI es considerarla como la disciplina que analiza problemas éticos que son creados por la tecnología de las computadoras o también los que son transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información. Algunos de los autores se plantean si la cambiante sofisticación tecnológica plantea nuevos dilemas éticos o si las cuestiones éticas permanecen constantes.

Otras definiciones de la EI son mucho más amplias. No se reducen a un nuevo campo de ética aplicada sino que, por ejemplo, en el libro de James Moor[6], la EI es el análisis de la naturaleza y el impacto social de la tecnología informática y la correspondiente formulación y justificación de políticas para un uso ético de dicha tecnología. La EI estaría relacionada con los problemas conceptuales y los vacíos en las regulaciones que ha ocasionado la tecnología de la información. El problema es que hay una falta de reglamentación en cómo utilizar estas nuevas tecnologías que posibilitan nuevas actividades para las cuales no hay o no se perciben con nitidez principios de actuación claros. Las personas con responsabilidades en el área de diseño o gestión de sistemas de información cada vez han de tomar más decisiones sobre problemas que no se resuelven con lo legal y lo cuasi-legal (reglamentos, manuales de procedimiento de las empresas, etc.) sino que rozan lo ético mismo. La tarea de la EI es aportar guías de actuación cuando no hay reglamentación o cuando la existente es

[3] Garza de Flores, Ética, 1993 Ed. Alhambra Mexicana.
[4] Lozano V, Rodríguez, Ética, Ed. Alhambra Mexicana, 1986.
[5] Dr.Emma Godoy, ¿Qué son y para qué sirven los valores?
[6] MOOR, James H., "What is Computer Ethics?", *Metaphilosophy*, Vol. 16, No. 4, October 1985, pp. 265-275.

obsoleta. Al vacío de políticas se añade generalmente un problema de vacío conceptual. Por ello la EI también ha de analizar y proponer una marco conceptual que sea adecuado para entender los dilemas éticos que ocasiona la informática.

Otra definición más general viene de Terrel Bynum, que basándose en Moor, define la EI como la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales. Estos valores afectados son la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal. En este concepto de EI se quieren incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de las computadoras, la evaluación social de las tecnologías o el derecho informático.

Códigos Deontológicos en Informática.

La Deontología (Del Griego *Deón* (deber) y *Logos* (razonamiento o ciencia): *Ciencia del Deber*), es la disciplina que trata lo concerniente a los deberes que corresponden a ciertas situaciones personales y sociales.

Originada en las profesiones intelectuales de antiguo origen histórico (Derecho, Medicina) la Deontología, en particular, denota el conjunto de reglas y principios que rigen determinadas conductas de los profesionales, ejercidas o vinculadas, de cualquier manera, al ejercicio de la profesión y a la pertenencia al respectivo grupo profesional.

Las asociaciones de profesionales de informática y algunas empresas relacionadas con la informática han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:

- Existan normas éticas para una profesión, esto quiere decir que un profesional, en este caso un técnico, no es sólo responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Sirven como un instrumento flexible, como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas comparadas con la velocidad del desarrollo de las tecnologías de la información. Los códigos hacen de la ley su suplemento y sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concientización pública, ya que crear unas normas así, hace al público consciente de los problemas y estimula un debate para designar responsabilidades.
- Estas normas tienen una función sociológica, ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de sus estatus profesional y parte de su definición como profesionales.
- Estas normas sirven también como fuente de evaluación pública de una profesión y son una llamada a la responsabilidad que permiten que la sociedad sepa qué pasa en esa profesión; aumenta la reputación del profesional y la confianza del público.
- En las organizaciones internacionales, estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales.

Los códigos son un paso en la concientización de las sociedades y organizaciones que quieren mejorar situaciones en las que los impactos sociales del desarrollo tecnológico no se tienen en cuenta. No tienen que duplicar lo que ya existe en la ley. La *ley* trata de la legalidad de las prácticas sociales, es normativa por definición y se impone con sanciones. Los *códigos*, en cambio, tratan del comportamiento según principios éticos, su normatividad es mostrar una declaración de intenciones sobre la "misión" de una institución y la coerción real con que se imponen es pequeña, aunque en algunos casos se incluyen expulsiones de la asociación en cuestión. La ley es el acercamiento de más poder normativo y asigna con claridad los derechos, responsabilidades y deberes de cada uno.

Un Código de ética se suma a un cambio de actitud por parte de la sociedad, respetando el accionar de la misma.

Situación actual de la Ética de la Informática

- La literatura existente es más sociológica que ética; es menos prescriptiva o normativa que descriptiva. En general no se ofrecen principios de actuación o respuestas a las preguntas "debe" (qué debería hacer yo como persona, que debería hacer yo y los míos como organización, qué normas sociales deberíamos promover, que leyes debemos tener...). El objetivo de la EI no es solamente proponer análisis sobre "sociología de la informática" o sobre la evaluación social de las tecnologías (technology assessment), sino ir algo más allá en el sentido de proporcionar medios racionales para tomar decisiones en temas en los que hay en juego valores humanos y dilemas éticos.

CÓDIGOS DE ÉTICA

En México, existen algunos códigos de ética sobre todo en el ámbito periodístico, en el derecho y la medicina. Sin embargo, hay instituciones educativas y empresas que se preocupan por tener un código de ética; en cuanto a seguridad informática son muy pocos, es por eso que propondremos una código de ética para la Facultad de Ingeniería.

Algunos de los códigos de ética que hacen referencia a la seguridad informática o a la informática, son los siguientes:

- Código de Ética del Ingeniero Mexicano (UMAI)
- Código de Ética de la IEEE
- American Society for Industrial Security (ASIS)
- Código de Ética de la Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C. (AMIPCI)

Se anexa el código de ética universitario, como una muestra de que la UNAM se preocupa porque la gente que labora en ella esté comprometida a realizar su trabajo apegado a los principios establecidos en este código de ética.

Para el personal involucrado en los áreas de sistemas informáticos seguirán el

CÓDIGO DE ÉTICA UNIVERSITARIO *y el* CÓDIGO DE ÉTICA PARA LA FACULTAD DE INGENIERIA EN EL ÁMBITO INFORMÁTICO.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CÓDIGO DE ÉTICA UNIVERSITARIO

A LA COMUNIDAD UNIVERSITARIA

Considerando que la Universidad Nacional Autónoma de México, como organismo descentralizado del estado, está comprometida con una responsabilidad moral y ética en el sentido de actuar de acuerdo a normas y principios que rijan la conducta del buen vivir de su comunidad.

Que esa responsabilidad ética obliga a una continua evaluación del comportamiento social y público de sus funcionarios y empleados, a fin de garantizar en todo momento el respeto al derecho y la observancia de su Normatividad evitando con ello faltas a las normas éticas que pongan en riesgo la estabilidad de la institución.

Que para fortalecer la confianza de la comunidad universitaria, así como la del pueblo de México, es preciso adoptar medidas tendientes a reforzar la grandeza de la institución, haciéndolos sentir parte importante de la misma, además de propiciar que sus labores no vulneren los principios de una ética institucional.

Se emite el presente Código de Ética para los funcionarios y empleados universitarios cuya implementación, es de trascendental importancia para esta Universidad.

ALCANCE Y OBJETIVO DEL CÓDIGO

Reglamentar la conducta de los funcionarios y empleados universitarios y, en general, a toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la administración universitaria.

PRINCIPIOS FUNDAMENTALES

I. Todo funcionario y empleado universitario considerará un deber, desempeñar su trabajo en apego a este Código de Ética.

II. Todo funcionario y empleado universitario, para apoyar y promover el honor y la dignidad de la institución con las normas más elevadas de la ética deberá:

a) Interesarse en el bienestar común y aplicar sus conocimientos profesionales para beneficio de la institución así como de sus integrantes.
b) Desarrollar sus deberes con honestidad e imparcialidad y servir con dedicación a sus superiores, sus empleados y a la comunidad universitaria general.
c) Reconocer que la trayectoria universitaria es el origen de una disponibilidad económica que debe permitir vivir con decoro, procurando asegurar para los suyos los recursos materiales y los elementos morales que le sean indispensables para su progreso y bienestar.
d) Esforzarse por aumentar la competencia y prestigio de los trabajadores y empleados universitarios en todas sus actividades.

POSTULADOS

I. Responsabilidad hacia la sociedad en general

Bien común: Asumo un compromiso irrenunciable con el bien común, entendiendo que la Universidad es patrimonio de la Nación, que sólo se justifica y legitima cuando se procura ese bien común, por encima de los intereses particulares.

Imparcialidad: Actuaré siempre en forma imparcial, sin conceder preferencias o privilegios indebidos a persona alguna.

Vocación de Servicio: Entiendo y acepto que trabajar para esta Universidad constituye al mismo tiempo el privilegio y el compromiso de servir a la sociedad, porque es ella quien contribuye a pagar mi salario.

Liderazgo: Promoveré y apoyaré estos compromisos con mi ejemplo personal, abonando a los principios morales que son base y sustento de una sociedad exitosa en institución ordenada y generosa.

Dignidad con la sociedad: Respetaré en el debate y en la toma de decisiones, la dignidad de las personas, siendo justo, veraz y preciso en mis apreciaciones, reconociendo la legítima diversidad de opiniones.

II. Responsabilidad hacia la comunidad universitaria

Honradez: Nunca usaré mi cargo para ganancia personal, ni aceptaré prestación o compensación alguna a mis remuneraciones a las que tengo derecho, de ninguna persona u organización que me pueda llevar a actuar con falta de ética mis responsabilidades y obligaciones.

Justicia: Ceñiré mis actos a la estricta observancia de la Normatividad Universitaria, impulsando una cultura de procuración efectiva de justicia y de respeto a la Institución.

Transparencia: Acepto demostrar en todo tiempo y con claridad suficiente, que mis acciones como funcionario y empleado universitario se realizan con estricto y permanente apego a las normas y principios de la Institución, fomentando su manejo responsable y eliminando su indebida discrecionalidad.

Rendición de cuentas: Proveeré la eficacia y la calidad en la gestión de la administración universitaria, contribuyendo a su mejora continua y a su modernización, teniendo como principios fundamentales la optimización de sus recursos y la rendición de cuentas.

Respeto: Respetaré sin excepción alguna la dignidad de la persona humana y los derechos y libertades que le son inherentes, siempre con trato amable y tolerancia para toda la comunidad universitaria.

Lealtad: Afirmo que todos mis actos se guían e inspiran por exaltar a la institución y a sus símbolos; así como el respeto a su Ley Orgánica y demás Normatividad que de ella emana y por la más firme creencia en la dignidad de la persona humana.

Responsabilidad: Acepto estar preparado para responder de todos mis actos de manera que la comunidad universitaria y la gente con que trato en particular, aumenten permanentemente su confianza en mí y en nuestra capacidad de servirles.

Competencia: Reconozco mi deber de ser competente, es decir, tener y demostrar los conocimientos y actitudes requeridos para el ejercicio eficiente de las funciones que desempeño, y actualizarlos permanentemente para aplicarlos al máximo de mi inteligencia y de mis esfuerzo.

Efectividad y Eficiencia: Comprometo la aplicación de mis conocimientos y experiencias de la mejor manera posible, para lograr que los fines y propósitos de la Universidad se cumplan con óptima calidad y en forma oportuna.

Manejo de recursos: todos los recursos propiedad de la Universidad sin importar su origen, los aplicaré únicamente para la consecución de los objetivos institucionales.

Calidad del personal: Contrataré para los cargos de mi dependencia, sólo a quienes reúnan el perfil para desempeñarse con rectitud, aptitud y la actitud necesarios.

III. Responsabilidad hacia los compañeros de trabajo

Valor civil: Reconozco mi compromiso de ser solidario con mis compañeros y conciudadanos; pero admito mi deber de denunciar y no hacerme cómplice de todo aquel que contravenga los principios éticos y morales contenidos en este instrumento.

Igualdad: Haré regla invariable de mis actos y decisiones el procurar igualdad de oportunidades para todos los universitarios, sin distingo de sexo, edad, raza, credo, religión o preferencia política.

Probidad: Declaro que todos los recursos y fondos, documentos, bienes y cualquier otro material confiado a mi manejo o custodia debo tratarlos con absoluta probidad para conseguir el beneficio colectivo.

Diálogo: Privilegiaré el diálogo y la concertación en la resolución de conflictos.

CÓDIGO DE ÉTICA PARA LA FACULTAD DE INGENIERIA EN EL ÁMBITO INFORMATICO.

1. Aplicación del código

El presente código de ética establece algunos puntos que regularán la conducta y el desempeño profesional de las personas encargadas de la seguridad informática de la Facultad de Ingeniería, a las cuales definiremos como Administradores de red (y de sistemas), independientemente del sistema operativo que utilicen; incluyendo a las personas que laboran en cualquier área de sistemas, sin importar el puesto que ocupen.

2. Actitud profesional

La excelencia técnica y ética de los administradores de red se vuelve indispensable para todos los profesionales de esta área, por lo que es necesario que ellos promuevan la difusión y práctica de los principios expresados en este código.

Los Administradores de red tienen la obligación de regir su conducta de acuerdo a las reglas contenidas en este código, las cuales deben considerarse mínimas pues se reconoce la existencia de otras normas de carácter legal y moral que amplían el de las presentes.

Este código rige la conducta de los Administradores de Red, así como el de las personas que pertenecen a cualquier área de sistemas, en sus relaciones con el público en general, con quien presta sus servicios (usuarios) y con sus compañeros de trabajo.

Los Administradores de red y las personas que trabajan en el área de sistemas, deben abstenerse de hacer comentarios sobre sus compañeros de trabajo o usuarios, que perjudiquen su reputación o el prestigio de su profesión, a menos que se soliciten por quién tenga un interés legítimo de ellos.

3. Actitud personal

Los Administradores de red y las personas que trabajan en el área de sistemas deben respeto a toda persona y su comportamiento tanto en lo personal como en lo social, debe atender a la práctica de buenas costumbres y seguir un objetivo útil.

Los Administradores de red y las personas que trabajan en el área de sistemas deben tener la costumbre de cumplir los compromisos adquiridos, no por el hecho de estar escritos, sino por convicción propia.

Los Administradores de red y las personas que trabajan en el área de sistemas deben de respetar y hacer respetar su tiempo y el de los demás, predicar con el ejemplo, poseer espíritu de servicio y habilidad para comunicarse con los demás.

Los Administradores de red y las personas que trabajan en el área de sistemas siempre actuarán cuidando el no afectar la integridad física, emocional ni económica de las personas.

4. Calidad profesional en el trabajo

Los Administradores de red y las personas que trabajan en el área de sistemas, deben realizar un trabajo de calidad en cualquier servicio que ofrezcan.

5. Preparación y calidad profesional

Por ser la información un recurso difícil de manejar, se requiere de Administradores de definan estrategias para su generación, administración y difusión; por lo que ninguna persona que no esté relacionada con la informática, computación o sistemas computacionales, que no cuente con experiencia y con la capacidad necesaria para realizar éstas actividades de manera satisfactoria y profesional, por ningún motivo podrá llevar a cabo esta actividad.

Los Administradores de red y las personas que trabajan en el área de sistemas, se preocuparán de que su propia actualización y capacitación profesional sea de crecimiento permanente.

6. Práctica de la profesión

Los Administradores de red y las personas que trabajan en el área de sistemas, deben analizar cuidadosamente las verdaderas necesidades que puedan tenerse de sus servicios, para proponer aquellas que más convengan dependiendo de las circunstancias.

Responsabilidades hacia el usuario

1. Importancia del usuario

El principal objetivo de los Administradores de la red y las personas que trabajan en el área de sistemas es la atención adecuada al usuario, al cual se le debe brindar todo el respeto .

2. Proteger el interés del usuario

Los Administradores de red y las personas que trabajan en el área de sistemas, deben aprovechar las herramientas (software, equipo de cómputo) adquiridas por la Facultad para el beneficio no sólo de ella sino también de los usuarios.

Los Administradores de Red deben asegurarse del buen uso de los recursos informáticos, evitando el mal uso para el que no fueron planeados y autorizados.

3. Responsabilidad profesional

Los Administradores de red y las personas que trabajan en el área de sistemas expresarán su opinión en los asuntos que se les hayan encomendado, teniendo en cuenta los principios expresados en éste código.

Deberán ser objetivos, imparciales en la emisión de sus opiniones o juicios, buscando siempre el beneficio de la institución de sus compañeros y usuarios.

4. Acceso a la información

Los Administradores de red y las personas que trabajan en el área de sistemas respetarán la información de carácter privado relativa a las personas, contenida en las bases de datos, excepto cuando se requiera una investigación por un incidente de seguridad o una investigación de carácter legal.

5.- Discreción profesional

Los Administradores de red y las personas que trabajan en el área de sistemas tienen la obligación de guardar discreción en el manejo de la información que se les ha proporcionado para poder prestar sus servicios. Considerar como confidencial toda la información que le ha sido confiada.

Los Administradores de red y las personas que trabajan en el área de sistemas no deben permitir el acceso a la información a personal no autorizado, ni utilizar para beneficio propio la información confidencial de los usuarios.

6.- Honestidad profesional.

Los Administradores de red y las personas que trabajan en el área de sistemas, no podrán modificar o alterar la información que se les ha confiado, para beneficio propio o de terceros, ni con fines de encubrir anomalías que afecten directamente los intereses de la Institución.

Los Administradores de red y las personas que trabajan en el área de sistemas no deben participar en actos que se califiquen de deshonestos.

7. No usar equipo de cómputo ni programas de la Institución para beneficio personal

Los Administradores de red y las personas que trabajan en el área de sistemas no deben usar el equipo de cómputo para fines de esparcimiento que afecten su desempeño profesional, aún cuando tenga la autorización para utilizar el equipo. Ni fomentar que personas ajenas a la Institución ingresen a las instalaciones y utilicen el equipo y los programas del software.

8. Trato adecuado a los usuarios y compañeros de trabajo

Los Administradores de red y las personas que trabajan en el área de sistemas deben tratar con respeto a todas las personas sin tener en cuenta raza, religión, sexo, orientación sexual, edad o nacionalidad.

Los directivos de las áreas de sistemas debe dar a sus colaboradores el trato que les corresponde como profesionales y vigilarán su adecuada superación profesional.

9. Finalización del trabajo

Al finalizar un proyecto independientemente del área de la que lo solicite, debe cumplir con todos los requisitos de funcionalidad, calidad y documentación pactados inicialmente, a fin de que se pueda obtener el mayor beneficio en la utilización de los mismos.

Los Administradores de red y las personas que trabajan en el área de sistemas deben cuidar que el equipo de cómputo y los programas propiedad de la Unidad se conserven en buen estado para su uso y aprovechamiento.

Al concluir el trabajo para el cual fue contratado, Los Administradores de red y las personas encargadas del desarrollo de sistemas en la Institución deben implementar los mecanismos necesarios, para que tenga la posibilidad de continuar haciendo uso de los programas de aplicación, así como de modificarlos, a pesar de su ausencia.

10. Desarrollo de sistemas

Las personas encargadas del desarrollo de sistemas en Institución deben determinar perfectamente el alcance del sistema y los requerimientos necesarios para su desarrollo.

Las personas encargadas del desarrollo de sistemas en la Institución deben determinar de manera clara la entrega de las diferentes etapas de desarrollo y establecer las fechas y compromisos formales de entrega, de cada una de las personas que participen en el desarrollo del sistema.

Las personas encargadas del desarrollo de sistemas en la Institución deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado que permita tomar decisiones.

Las personas encargadas del desarrollo de sistemas en la Institución deben dejar siempre documentado el sistema desarrollado, con todos los detalles necesarios, de tal manera que con su consulta se conozca el funcionamiento del sistema.

Las personas encargadas del desarrollo de sistemas en la Institución deben tener la capacidad para reconocer sus fallas en las revisiones, hacer correcciones y aclarar las dudas de quien solicito el sistema, así como proponer posibles alternativas de solución.

Las personas encargadas del desarrollo de sistemas en la Institución deben comunicar los problemas que se les vayan presentando.

RESPONSABILIDAD HACIA LA PROFESIÓN

1. Respeto a sus compañeros de trabajo y a su profesión

Los Administradores de red y las personas que trabajan en el área de sistemas cuidarán las relaciones que sostienen con sus compañeros de trabajo y colegas, buscando mejorar el ambiente de trabajo y fomentar el trabajo en equipo.

Los Administradores de red y las personas que trabajan en el área de sistemas deberán basar su reputación en la honestidad, honradez, lealtad, respeto, laboriosidad y capacidad profesional, observando las reglas de ética más elevadas en sus actos y evitando toda publicidad con fines de lucro o auto elogio.

Buscarán la manera de hacer cumplir y respetar este código de ética; además de fomentar la adopción de un código de ética.

2. Difusión y enseñanza de conocimientos

Los Administradores de red y las personas que trabajan en el área de sistemas deben mantener altas normas profesionales y de conducta, especialmente al transmitir sus conocimientos, logrando contribuir al desarrollo y difusión de los conocimientos de su profesión.

3. Especialización profesional de los Administradores del Sistema

Los Administradores de red y las personas que trabajan en el área de sistemas deben tener una orientación hacia cierta rama de la informática, computación o sistemas computacionales, debiéndose mantener a la vanguardia en el área de conocimiento de su interés.

4. Competencia profesional

Los Administradores de red y las personas que trabajan en el área de sistemas mantener actualizados todos los conocimientos inherentes a las áreas de su profesión así como participar en la difusión de estos conocimientos a otros miembros de la profesión.

Los Administradores de red y las personas que trabajan en el área de sistemas deben informarse permanentemente sobre los avances de la informática, la computación y los sistemas computacionales.

5. Evaluación de capacidades

Los Administradores de red y las personas que laboran en sistemas en la Institución deben autoevaluarse periódicamente con la finalidad de determinar si cuentan con los conocimientos suficientes para ofrecer un trabajo de calidad.

En caso de que los Administradores de red y las personas que laboran sistemas en la Institución tengan personas a su cargo deberán asegurarse de que sean evaluados sus conocimientos periódicamente.

6. Personal a sus servicios

Los Administradores de los Sistemas y las personas encargadas del desarrollo de sistemas en la Institución deben realizar una supervisión del desempeño de las personas que colaboran con ellos en el desarrollo de sistemas.

7. Práctica docente

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben cumplir con su responsabilidad en asistencia y puntualidad en el salón de clases.

Evaluaciones a los alumnos

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben comunicar los procedimientos de evaluación durante el tiempo que dure la enseñanza.

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos deben llevar a cabo las evaluaciones en las fechas determinadas y entregar los resultados en un tiempo adecuado, así como también hacer una revisión total del examen y aclarar todas las dudas que resulten derivadas de su aplicación.

Los Administradores de red o instructores y las personas que pertenecen a Institución que den clases en la Facultad de Ingeniería o que den cursos llevar una supervisión del desempeño del alumno en forma personal preocupándose por establecer si los bajos resultados son resultado del desempeño del alumno o del profesor o instructor.

GLOSARIO

Sitio

Cualquier organización (militar, gubernamental, comercial, académica, etc.) que posea recursos relativos a redes y computadoras.

Usuario

Cualquier persona que hace uso de alguno de los recursos de cómputo con los que cuenta una organización.

Administrador

El responsable de mantener en operación continúa los recursos de cómputo con los que cuenta un sitio

Seguridad en cómputo

Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autentificados por mecanismos de control de acceso y sujetos a auditoria.

- Confidencial: La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.
- Íntegro: La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo.
- Consistente: el sistema, al igual que los datos, debe comportarse como uno espera que lo haga.
- Disponible: La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.
- Autentificado: Únicamente deben ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.
- Control de acceso: Debe conocer se en todo momento quién entra al sistema y de dónde procede.
- Auditoria: Deben conocerse en cada momento las actividades de los usuarios dentro del sistema.

Incidente

Un evento que pone en riesgo la seguridad de un sistema de cómputo.

Ataque

Un incidente cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada.

Firewall

Un dispositivo de hardware y software que actúa como una barrera protectora entre una red privada y el mundo exterior; se usa para proteger el acceso a los recursos internos desde el exterior, así como para controlar los recursos externos que son accedidos desde la red privada.

Herramientas de seguridad

Programas que nos permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas, casi todas de libre distribución. Algunos ejemplos de herramientas de seguridad a considerar para implementar un esquema de seguridad son:

- Para el manejo de contraseñas: anipasswd, passwd+, crack, John The Ripper, S/Key
- Para el manejo de autenticación: Kerberos, SecureRPC
- Para el monitoreo de redes: Satan, ISS
- Para auditoría interna: COPS, Tiger, Tripwire
- Para control de acceso: TCP-Wrapper, PortSentry

SPAM

Mensaje de correo electrónico no solicitado por el receptor, usualmente distribuido a una lista de direcciones y cuyo contenido generalmente es publicidad de productos o servicios.

DHCP

DHCP (Dinamic Host Configuration Protocol) es una extensión del protocolo BOOTP (BOOTP habilita a clientes disskless a inicializar y automáticamente configurar TCP/IP). DHCP centraliza y administra la información de la configuración de TCP/IP, automáticamente asigna direcciones IP a las computadoras configuradas para utilizar DHCP.

SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

IDS es la abreviatura de Sistema de Detección de Intrusos (por sus siglas en inglés), que es el arte de detectar actividad inapropiada, incorrecta o anónima. Los sistemas de Detección de Intrusos que operan en un host para detectar actividad maliciosa se les conoce como Sistemas de Detección de Intrusos para host y los sistemas DI que operan en el flujo de datos de una red se les conoce como sistemas de Detección de Intrusos para red.

GLOSARIO

AppleTalk	Una arquitectura de red local (LAN) que se incorporó en las computadoras Apple de Macintosh e impresoras de láser. AppleTalk soporta el esquema de cableado LocalTalk de Apple, así como Ethernet y el Token Ring de IBM. Se puede conectar computadoras de Macintosh e impresoras, y aún PC´s aun equipados con hardware especial AppleTalk y software.
ARP	Address Resolution Protocol (Protocolo de Resolución de Dirección), es un protocolo de capa de red que solía convertir una dirección IP en una dirección física (llamado dirección DLC), como una dirección de Ethernet. Un host que desea obtener una dirección física difunde una petición de ARP en la red de TCP/IP. El anfitrión sobre la red que tiene la dirección de IP en la petición y entonces contesta con su dirección de hardware física.
Broadcast	Simultáneamente enviar el mismo mensaje a múltiples recipientes. La difusión es una característica útil en los sistemas del correo electrónico. En la interconexión, una distinción es hecha entre el broadcasting y el multicasting. El broadcasting envía un mensaje a cada uno sobre la red mientras que el multibastidor envía un mensaje a una lista escogida de recipientes.
CGI	Common Gateway Interface (Interfaz de Entrada Común). Una especificación para transferir información entre un servidor WWW y un programa CGI. Un programa CGI es cualquier programa diseñado para aceptar y devolver los datos que se conforman a la especificación CGI. El programa podría ser escrito en cualquier lenguaje de programación, incluyendo C, Perl, Java o Visual Basic.
Comunicación Full-Duplex	Se refiere a la transmisión de datos en dos direcciones simultáneamente. Por ejemplo, un teléfono ya que en ambos nodos se puede hablar inmediatamente.
Comunicación Half-Duplex	Se refiere a la transmisión de datos justamente en una dirección a la vez. Por ejemplo, un transmisor-receptor portátil es un dispositivo medio duplex porque sólo un nodo puede hablar a la vez.
Comunicación Simplex	Se refiere a la transmisión en sólo una dirección. Simplex se refiere a comunicaciones de dirección única donde un nodo es el transmisor y el otro es el receptor. Un ejemplo de comunicaciones simplex es una radio simple, puede recibir datos de estaciones, pero no puede transmitir datos.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DECNET	DECnet es un grupo de productos de comunicaciones de datos, que incluye una suite de protocolos, desarrollado y apoyado por Digital Equipment Corporation. La primera versión de DECNET, se liberó en 1975, permitió conectar directamente dos minicomputadoras PDP-11 para comunicarse.

DLC — Data Link Control (Control de Enlace de transmisión). Es la segunda capa más baja en el Modelo de Referencia OSI. Cada tarjeta de interfaz de red (NIC) tiene una dirección de DLC o el identificador DLC (DLCI) que únicamente identifica el nodo sobre la red. Algunos protocolos de red, como Ethernet y Token Ring usan las direcciones de DLC exclusivamente. Otros protocolos, como TCP/IP, usan una dirección lógica en la Capa de Red para identificar nodos. En última instancia, todas las direcciones de red deben ser traducidas a direcciones de DLC. En redes TCP/IP, esta traducción es realizada con el Protocolo de Resolución de Dirección (ARP).
Para las redes que se conforman al estándar IEEE 802 (e.g., Ethernet), la dirección DLC es por lo general llamada dirección de Control de Acceso al Medio (MAC).

DNS — Domain Name System (or Service or Server). Un servicio de Internet que traduce nombres de dominio en direcciones IP. Como los nombres de dominio son alfabéticos, ellos son más fáciles para recordar. La Internet sin embargo, está realmente basada en direcciones IP. Siempre que se usa un nombre de dominio, un servicio de DNS debe traducir el nombre en la correspondencia dirección IP. Por ejemplo, el nombre de dominio www.example.com podría traducir a 198.105.232.4.

FDDI — Fiber Distributed Data Interface, es un juego de protocolos ANSI para enviar datos digitales sobre la fibra óptica. Las redes FDDI son redes Token Passing, y soporta transferencia de datos de hasta 100 Mbps. Las redes FDDI típicamente son usadas como backbone para redes de área amplia.
Una extensión a FDDI, llamada FDDI-2, apoya la transmisión de voz, vídeo y datos. Otra variación de FDDI, llamada Tecnología FDDI Full Duplex (FFDT) usa la misma infraestructura de red, pero potencialmente puede soportar transferencia de datos de hasta 200 Mbps.

FTP — File Transfer Protocol (Protocolo de Transferencia de Archivo), el protocolo para cambiar archivos sobre la Internet. FTP trabaja de la misma manera como HTTP para transferir páginas Web de un servidor al navegador de un usuario y SMTP para transferir el correo electrónico a través de la Internet . FTP usa los protocolos TCP/IP de Internet para permitir la transferencia de datos.

GNU — GNU's not UNIX. Es un software compatible con UNIX desarrollado por la Free Software Foundation (FSF). La filosofía detrás de GNU es producir software no propietario. Cualquiera lo puede descargar, modificar y redistribuir. La única restricción es que no se puede limitar la redistribución. Este proyecto inicio en 1983 en el Massachusetts Institute of Technology.

GPL	General Public License (Licencia Publica General). Es la licencia que acompaña algunos programas (software) de código abierto en la que detalla como el software y sus complementos pueden libremente copiados. El GPL no cubre otras actividades que el copiar, la distribución y la modificación del código original.
HDLC	Control de enlace de datos de alto nivel. Es un protocolo de transmisión usado en la capa de enlace de transmisión (Capa 2) del OSI modelo de capas para comunicaciones de datos. El protocolo HDLC integra la información en un marco de datos que permite a dispositivos para controlar el flujo de datos y errores correctos. HDLC es un estándar ISO desarrollado por el Control de Enlace de Transmisión Sincrónico (SDLC) propuesto por IBM en los años 70´s.
HTTP	HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto), el protocolo subyacente usado por el World Wide Web. HTTP define como los mensajes son formateados y transmitidos, y que acciones realizaran los servidores Web y los navegadores.
ICMP	Internet Control Message Protocol (Protocolo de Mensaje de Control de Internet), una extensión al Protocolo de Internet (IP) definido por el RFC 792. ICMP soporta paquetes que contienen el error, control y mensajes informativos. El comando PING, por ejemplo, usa ICMP para probar una conexión a Internet.
IEEE	Instituto de Eléctricos e Ingenieros Electrónicos. IEEE es una organización compuesta de ingenieros, científicos, y estudiantes. El IEEE es el mejor conocido por desarrollar normas para la industria de electrónica y la computación.
IMAP	Internet Message Access Protocol (Protocolo de Acceso de Mensaje de Internet), un protocolo empleado para recuperar mensajes electrónicos. La última versión, IMAP4, es similar a POP3, pero soporta algunas características adicionales.
IP	Internet Protocol (Protocolo de Internet). IP especifica el formato de paquetes, también llamados datagramas, y el esquema de direccionamiento. La mayor parte de redes combinan IP con un protocolo de nivel más alto el Protocolo de Control de Transmisión (TCP), que establece una conexión virtual entre los nodos destino y fuente.
IPG	Inter Packet Gap
Ipng	vease IPv6
IPv6	Protocolo de Internet Siguiente Generación, una versión del Protocolo de Internet (IP) en revisión por los comités de estándares IETF para sustituir la versión 4 del IP. El nombre oficial de IPNG es IPV6, donde el v6 significa la versión 6. La versión actual de IP es la versión 4. Entre las características

mas fundamentales que podemos encontrar en este nuevo protocolo son:

- Mayor espacio de direcciones.
- Seguridad intrínseca en el núcleo del protocolo. (IPsec) Calidad de servicio (QoS) y Clase de servicio (CoS).
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65535 bytes.

IPX — Internet Packet Exchange. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

ISDN — Integrated Services Digital Network. Red Digital de Servicios Integrados. Un estándar de comunicaciones internacional para enviar voz(voto), vídeo, y datos sobre líneas telefónicas digitales o cables normales telefónicos. ISDN apoya las tarifas de transferencia de datos de 64 Kbps (64,000 añicos por segundo).

ITU — International Telecommunication Union (Unión de Telecomunicación Internacional) una organización intergubernamental por la cual organizaciones públicas y privadas desarrollan telecomunicaciones. Es responsable de adoptar tratados internacionales, regulaciones y normas telecomunicaciones.

LAN — Local Area Network. Red de área local. Es un segmento de red con estaciones de trabajo o nodos y servidores enlazados, o un conjunto de segmentos de red interconectados, por lo general dentro de la misma área, como por ejemplo un edificio.

MAC — Una dirección de hardware que identifica en forma única cada nodo de una red. En IEEE redes 802, el Control de Enlace de transmisión (DLC) la capa del Modelo de Referencia de OSI son divididas en dos subcapas: la capa de Control de Eslabón Lógico (LLC) y la capa de Control de Acceso de Medios (MAC). La capa MAC interviene directamente con el medio de red. Por consiguiente, cada tipo diferente del medio de red requiere una capa MAC diferente.

Mbps — Mega Bits por Segundo. Medida de velocidad de transferencia de información.

MIB — Management Information Base (Administración de Información Base). Es una base de datos de objetos que pueden ser monitoreados por un sistema administrador de redes. Ambos, el SNMP y el RMON, usan el formato estándar MIB que permite a cualquier herramienta SNMP y RMON monitorear cualquier dispositivo definido por un MIB

MPLS	Multiprotocol Label Switching. El MPLS representa la interacción más inteligente entre IP - ATM, en una arquitectura distribuida, donde se obtiene lo mejor de cada uno de los mecanismos, el enrutamiento IP combinado con la conmutación ATM, dentro de un posicionamiento óptimo de Red. MPLS provee las características en términos de escalabilidad y calidad de servicio que se espera tener hoy para las redes y servicios basados en IP.
Multicasts	Se refiere a enviar mensajes a un grupo selecto.
NAT	Network Address Translation (Traducción de Dirección de Red). Es un estándar de Internet que permite en una LAN usar el juego de direcciones IP para el tráfico interno y un segundo juego de direcciones para el tráfico externo. El NAT tiene tres objetivos principales: • Proporciona un firewall ocultando direcciones de IP internas. • Permite a una empresa usar direcciones IP internas. • Permite a una empresa combinar múltiples conexiones ISDN en una conexión a Internet.
NetBEUI	NetBios Extended User Interface. Es una versión perfeccionada del protocolo NetBIOS usado por sistemas de operativos para redes.
Netbios	Network Basic Input Output System (Sistema Básico de Entrada Salida), un API que aumenta el BIOS del DOS añadiendo funciones especiales para redes de área local (LAN). Casi todos las LAN para computadoras personales están basados en el NetBIOS. Es un protocolo que sirve para compartir archivos e impresoras en una red. NetBIOS es una especificación de interfaz para acceder a servicios de networking local
NFS	Network File System (Sistema de Archivos de Red) una aplicación cliente/servidor diseñado por Sun Microsystems que permite a todos los usuarios de red tener acceso a archivos compartidos almacenados sobre las computadoras de diferentes tipos. NFS provee el acceso a archivos compartidos por un interfaz llamado Sistema de Archivos Virtuales (VFS) que corre arriba de TCP/IP. Los usuarios pueden manipular archivos compartidos como si estos estuvieran almacenados sobre el propio disco duro del usuario. Con NFS, las computadoras conectadas a una red funcionan como clientes teniendo acceso a archivos remotos, y como servidores proporcionando el acceso de usuarios remoto a archivos locales compartidos.
NOC	Network Operation Center
Nodo	Un punto de procesamiento. Un nodo puede ser una computadora o cualquier otro dispositivo. Cada nodo tiene una dirección de red única, llamada dirección Data Link Control (DLC) o dirección Media Access Control (MAC).

OSI	Sistema de Interconexión Abierta, un estándar de ISO para las comunicaciones mundiales que define un marco de redes para poner en práctica siete capas de protocolos. El control es pasado de una capa a la siguiente, comenzando en la capa de aplicación, continuando hasta la capa inferior, sobre el medio al siguiente nodo y sostener la jerarquía.
P2P	Usualmente se refiere para simplificar el termino peer-to-peer. Es una especie de red en la cual cada estación de trabajo tienen capacidades y responsabilidades equivalentes. Esto se diferencia de arquitecturas cliente/servidor, en las cuales algunas computadoras son dedicadas para servir a las demás. Las redes peer-to-peer son generalmente más simples, pero por lo general no ofrecen el mismo funcionamiento bajo cargas pesadas. e.g. kazaa, napster.
POP	Post Office Protocol (Protocolo de Correo). Es un protocolo que suele recuperar el correo electrónico de un servidor de correo. Mayoría de los correos electrónicos (conocido como el cliente de un correo electrónico) usa el protocolo POP, aunque unos puedan usar el más reciente protocolo IMAP (Protocolo de Acceso de Mensaje de Internet).
PPP	Point-to-Point Protocol (Protocolo Punto-Punto), un método para conectar una computadora a Internet. PPP es más estable que el más viejo protocolo de RESBALÓN y proporciona el error que comprueba rasgos. Trabajando en la capa de enlace de transmisión del modelo de OSI, PPP envía los paquetes TCP/IP del ordenador a un servidor que los pone en la Internet.
proxy	Un servidor que esta entre la aplicación del cliente, como el Web browser, y un servidor real. Éste intercepta todas las solicitudes del servidor real para ver si puede realizar las solicitudes por si mismo. Si no, las redirecciona hacia el servidor real. Un servidor proxy tiene dos propósitos principales: Mejorar el desempeño y Filtrar las Solicitudes.
QoS	Calidad de Servicio
RMON	Remote Monitoring (Supervisión Remota). Es un protocolo de dirección de red que permite a la información de red ser juntada en solo una terminal de trabajo
SMTP	Simple Mail Transfer Protocol (Protocolo de Transferencia de Correo Simple). Es un protocolo para enviar mensajes electrónicos entre servidores. La mayor parte de los sistemas de correo electrónico que envían al correo sobre Internet emplean SMTP para enviar mensajes de un servidor al otro; desde donde el usuario puede recuperar su correo electrónico usando POP o IMAP.

Sniffer	Es un programa o dispositivo que monitorea la información que viaja en la red. Los sniffers pueden ser usados tanto para legitimizar la administración de la red como para extraer o robar información de la red. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de la red porque virtualmente son imposibles de detectar y pueden ser insertados dondequiera.
SNMP	Simple Network Management Protocol (Protocolo de Dirección de Red Simple). Un juego de protocolos para administrar redes complejas. Las primeras versiones de SNMP fueron desarrolladas a principios de los años 80. SNMP trabaja enviando mensajes, llamadas Unidades de Datos de Protocolo (PDU), a las diferentes partes de una red. Los dispositivos SNMP-compliant, llamados agentes, almacenan datos sobre ellos en Bases de Información de Dirección (MIB) y regresan estos datos a los solicitantes de SNMP.
TCP/IP	Transsmision Control Protocol/Internet Protocol. Protocolo de control de transmisión/protocolo Internet. Los protocolos definen las reglas de comunicación. TCP/IP se diseñó específicamente para la interconexión de diferentes tipos de equipos de computadoras.
Telnet	Un programa de emulación terminal para redes de TCP/IP como Internet. El programa Telnet corre desde una computadora y ésta se conecta a un servidor sobre la red. Una vez conectado se pueden ejecutar comandos como si estuviera directamente sobre la consola del servidor. Esto permite controlar al servidor y comunicarse con otros servidores sobre la red. Para comenzar una sesión Telnet, se debe conectar a un servidor validando username y contraseña.
Token	Es una serie especial de bits que viajan alrededor de una red. La señal actúa como un boleto, permitiendo a su propietario enviar un mensaje a través de la red. Hay sólo un token para cada red, por lo que no hay ninguna posibilidad que dos computadoras intentarán transmitir mensajes al mismo tiempo.
Token Passing	El Token Passing emplea un token, o serie de bits, para conceder un permiso de dispositivo de transmitir sobre la red. Cualquier dispositivo puede poner datos en la red. Cuando su transmisión es completada, el dispositivo pasa la señal a lo largo del siguiente dispositivo en la topología. El sistema gobierna en el protocolo cuanto tiempo un dispositivo puede mantener el token, cuanto tiempo lo puede transmitir y como generar un nuevo token.
TTL	Time To Live (Tiempo de Vida). Es un campo en el Protocolo de Internet (IP) que especifica cuántos más saltos un paquete puede viajar antes de ser desechado o devuelto.

UDP	User Datagram Protocol (Protocolo de Datagrama de Usuario). Un protocolo sin conexión que, como TCP, corre sobre la cima de redes de IP. A diferencia de TCP/IP, UDP/IP proporciona muy pocos servicios de recuperación de error, que ofrecen en cambio un modo directo de enviar y recibir datagramas sobre una red IP. Esto es usado principalmente para difundir mensajes sobre una red.
Unicast	La comunicación que ocurre sobre una red entre un remitente solo y un receptor solo
VLAN	Virtual Local Area Network (Red de Area Local Virtual). Es una forma sencilla de crear dominios virtuales de broadcast dentro de un ambiente de switch's independiente de la estructura física y tiene la habilidad para definir grupos de trabajo basados en grupos lógicos y estaciones de trabajo individuales, más que por la infraestructura física de la red. El tráfico dentro de una VLAN es switcheado por medios rápidos entre los miembros de la VLAN y el tráfico entre diferentes VLANs es reenviado por el ruteador.
WAN	Wide Area Network (Red de Área Amplia). Red de área amplia. Son redes que cruzan límites municipales, estatales e internacionales. Los enlaces se realizan con los servicios públicos y privados de telecomunicaciones, además con los enlaces por satélites y microondas. Las WAN están constituidas por redes LAN, de CAMPUS y MAN.

REFERENCIAS.

- Sterbenz, James P.G; High-speed networking: a systematic approach to high-bandwidth low-latency communication; Wiley Networking Council series, Whiley Computer Publishing, USA, 2001.
- Chowdhury, Dhiman Deb.; High Speed LAN technology handbook; Springer, Germany 2000
- Stamper, David A.; Local area networks; 3 ed.; Prentice Hall, New Jersey 2001.
- Stallings, William; Data and computer communications; 6 ed. Prentice Hall, New Jersey 2000.
- Stallings, William; Local and metropolitan area networks; 5 ed. Prentice Hall, New Jersey 1997.
- Deal, Richard A.; CCNP Swithcing Exam Cram; Coriolis, EEUU 2000
- Subramanian, Mani; Network Management. Principles and Practice; Addison-Wesley, EEUU, 2000.
- Hsu, John Y; Computer Networks. Architecture, Protocols and Software; Artech House, EEUU 1996.
- Held, Gilbert; Internetworking LAN´s and WAN´s; John Wiley & Sons, England, 1993
- Jenkins, Neil; Schatt, Stan; Redes de Área Local (LAN); 5° ed; Prentice Hall; México, 1996
- Tan, T.C.; Gigabit Ethernet and Structured Cabling; IEEE Electronics and Communication Engineering Journal, August 2000.
- EIA/TIA 568-A; Norma para Cableado de Telecomunicaciones en Edificios Comerciales, Telecommunications Industry Association, EEUU, 1995.
- EIA/TIA 569; Norma para vías de telecomunicaciones v espacios en edificios comerciales; Electronic Industries Association, Washington, 2000.
- www.ieee.org
- www.cudi.edu.mx
- www.internet2.unam.mx